Section de Mathématiques, Prof. Eva Bayer-Fluckiger

Projet de Semestre

Groupes de Brauer

Isaac Mabillard

Assistant Responsable : Klaas-Tido Rühl

1er janvier 2010

Table des matières

Introduction

Le but de ce projet est d'étudier une partie de la théorie associée aux algèbres centrales simples et, plus spécifiquement, aux groupes de Brauer sur un corps.

Notre premier objectif sera de démontrer le théorème de Wedderburn qui affirme qu'une algèbre simple de dimension finie est isomorphe à un anneau de matrices construit sur un corps gauche (déterminé à isomorphisme près). Dès lors, le problème de la classification des algèbres simples est réduit à la classification des corps gauches.

Un outil développé en vue de cette classification est le groupe de Brauer qui définit une structure de groupe sur l'ensemble (quotienté par une relation d'équivalence) des algèbres centrales simples.

On présentera une définition du groupe de Brauer et on étudiera son comportement dans le cas d'extensions de corps pour arriver à une caractérisation des algèbres centrales simples.

Suite à cela, on présentera une famille particulière d'algèbres : les quaternions. Sur eux, en utilisant des propriétés des formes quadratiques, on démontrera une règle de calcul dans le groupe de Brauer.

L'étude des algèbres et des modules sera l'objet du chapitre 1. Le chapitre 2 introduira le produit tensoriel d'algèbres. En l'utilisant, on pourra définir la loi de composition du groupe de Brauer qui sera décrit dans le chapitre 3, où on poursuivra également l'étude des algèbres.

Pour finir on introduira, dans le chapitre 4, les formes quadratiques et les quaternions, avant d'établir un lien entre l'équivalence d'espaces quadratiques et d'algèbres des quaternions. Dès lors, on pourra utiliser des propriétés liées aux formes quadratiques pour étudier les quaternions.

Chapitre 1

Algèbres et Modules

1.1 Définition. Une **algèbre** (**associative**) sur un corps F, ou F**-algèbre**, est un ensemble non-vide A, muni de trois opérations, appelées **addition** (notée par $+$), **multiplication** (notée par juxtaposition) et **multiplication scalaire** (aussi notée par juxtaposition), qui satisfont les propriétés suivantes :

(a) A est un espace vectoriel sur F sous l'addition et la multiplication scalaire.

(b) A est un anneau sous addition et multiplication, avec identité.

(c) Si $r \in F$ et $a, b \in A$, alors

$$r(ab) = (ra)b = a(rb).$$

Une algèbre est dite de **dimension finie** si elle est de dimension finie en tant qu'espace vectoriel. Une algèbre est dite **commutative** si A est un anneau commutatif. Un élément $a \in A$ est dit **inversible** s'il existe un élément $b \in A$ pour lequel $ab = ba = 1$.

Dans notre définition, nous avons demandé que A soit un anneau *avec identité*, une telle algèbre est appelée **algèbre unitaire**.

1.2 Définition. Une **sous-algèbre** B d'une F-algèbre A est un sous-ensemble de A qui soit un sous-anneau de A (avec la même identité que A) et un F-sous-espace vectoriel de A.

1.3 Définition. Le **centre** d'une F-algèbre A est l'ensemble

$$\mathcal{Z}(A) = \{a \in A \mid ax = xa \text{ pour tout } x \in A\}$$

de tous les éléments de A qui commutent avec chaque élément de A.

Le centre d'une F-algèbre A est toujours une sous-algèbre de A. En effet, $\mathcal{Z}(A)$ est un sous-anneau de A comme, pour tout $a, b \in \mathcal{Z}(A)$, on a

(a) $1 \in \mathcal{Z}(A)$ comme $1x = x1$ pour tout $x \in A$,

(b) $ab \in \mathcal{Z}(A)$ comme $abx = axb = xab$ pour tout $x \in A$,

(c) $a - b \in \mathcal{Z}(A)$ comme

$$(a-b)x = ax - bx = xa - xb = x(a-b)$$

pour tout $x \in A$,

et, de plus, $\mathcal{Z}(A)$ est un sous-espace vectoriel de A comme il est stable par addition (argument identique à (c) ci-dessus) et il est stable par multiplication scalaire comme, pour tout $a \in \mathcal{Z}(A)$, $x \in A$ et $\alpha \in F$, on a

$$(\alpha a)x = \alpha(ax) = \alpha(xa) = x(\alpha a),$$

i.e. $(\alpha a) \in \mathcal{Z}(A)$.

On remarque que le centre d'une algèbre n'est jamais trivial comme il contient toujours une copie de F :

$$\{r1 \mid r \in F\} \subseteq \mathcal{Z}(A).$$

En effet, on a vu que $1 \in \mathcal{Z}(A)$ et $\mathcal{Z}(A)$ est stable par multiplication scalaire.

1.4 Définition. Une F-algèbre A est dite **F-centrale** si son centre est réduit à la copie de F dans A :

$$\mathcal{Z}(A) = \{r1 \mid r \in F\},$$

La proposition suivante donne deux autres conditions équivalentes pour qu'une algèbre soit centrale.

1.5 Proposition. Soit A une algèbre sur un corps F. Alors les trois conditions suivantes sont équivalentes :

(a) A est F-centrale ;

(b) $\mathcal{Z}(A) \cong F$ en tant que F-espaces vectoriels ;

(c) $\dim_F(\mathcal{Z}(A)) = 1$.

Preuve. La vérification est immédiate. □

Nous n'avons pas demandé qu'une algèbre soit commutative, nous devons donc en tenir compte dans notre définition d'idéal.

1.6 Définition. Un **idéal à gauche** d'une algèbre A est un sous-groupe I de A pour l'addition, fermé sous multiplication *à gauche* par des éléments de A, *i.e.*

$$a \in A,\ i \in I \ \Rightarrow\ ai \in I.$$

Un **idéal à droite** d'une algèbre A est un sous-groupe de A pour l'addition, fermé sous multiplication *à droite* par des éléments de A.

Un sous-ensemble I de A est appelé **idéal bilatère** s'il est à la fois un idéal à gauche et un idéal à droite de A.

Un idéal de A est dit **propre** s'il est non-nul et différent de A.

On remarque que si un idéal (à gauche ou à droite) I d'une algèbre A contient 1, alors $I = A$.

1.7 Définition. Une algèbre est **simple** si

(a) Le produit dans A n'est pas trivial, *i.e.* $ab \neq 0$ pour au moins une paire d'éléments $a, b \in A$,

(b) A n'a pas d'idéal bilatère propre.

1.8 Définition. Une algèbre D sur un corps F est appelée **corps gauche** si $1_D \neq 0_D$ et si tout élément non-nul de D possède un inverse multiplicatif.

Nous avons déjà vu que le centre $\mathcal{Z}(D)$ d'une algèbre est un sous-anneau de D. Dans le cas d'un corps gauche, il s'agit en fait d'un corps. En effet, comme le centre d'une algèbre est toujours commutatif, il nous suffit de montrer que $\mathcal{Z}(D)$ est stable par passage à l'inverse pour conclure. Soit donc $a \in \mathcal{Z}(D)$ ayant pour inverse a^{-1} dans D et soit $x \in D$: on a que $ax = xa$ implique $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$, *i.e.* $xa^{-1} = a^{-1}x$, et donc $a^{-1} \in \mathcal{Z}(D)$.

Une deuxième propriété intéressante des corps gauches est qu'ils sont toujours simples. En effet, si I est un idéal bilatère non-zéro d'un corps gauche D, alors on peut choisir un élément inversible a dans I et on a, par définition des idéaux bilatères, que $1 = a^{-1}a \in I$, d'où on conclut directement que $I = D$, *i.e.* D n'a pas d'idéal bilatère propre.

1.9 Définition. Soit R un anneau avec identité. Un **R-module à gauche** (ou **module à gauche sur** R) est un ensemble non-vide M, muni de deux opérations. La première opération, appelée **addition** (notée par $+$), assigne à chaque couple $(u, v) \in M \times M$ un élément $u+v \in M$. La deuxième opération, appelée **multiplication scalaire** (notée par juxtaposition), assigne à chaque couple $(r, v) \in R \times M$ un élément $rv \in M$. De plus, les propriétés suivantes sont satisfaites :

(a) M est un groupe abélien pour l'addition.

(b) Pour tout $r, s \in R$ et $u, v \in M$ on a

$$\begin{aligned} r(u+v) &= ru + rv, \\ (r+s)u &= ru + su, \\ (rs)u &= r(su), \\ 1u &= u. \end{aligned}$$

L'anneau R est appelé **anneau de base** de M et ses éléments sont appelés **scalaires**.

La définition d'un **R-module à droite** est similaire à celle d'un R-module à gauche, à la différence que l'anneau R n'agit plus à gauche sur M, mais à droite.

Un ensemble M est appelé **module bilatère sur** R s'il est à la fois un module à gauche sur R et un module à droite sur R.

Un espace vectoriel est un type particulier de module : un module avec un corps comme anneau de base.

On peut toujours construire un R-module à gauche sur un idéal à gauche I d'un anneau R (avec identité). En effet, I est alors un groupe abélien pour l'addition, et comme I est un idéal à gauche, il est fermé par multiplication à gauche par un élément de R, *i.e.* par multiplication scalaire à gauche. Les autres conditions de la définition de module à gauche découlent directement du fait que R est un anneau. Une construction similaire permet de mettre une structure de module à droite sur un idéal à droite et de module bilatère sur un idéal bilatère.

1.10 Définition. Soit M un R-module à gauche. Un sous-ensemble $\mathcal{B}$ de M est une **base** s'il est linéairement indépendant et s'il engendre M par combinaisons linéaires. Un R-module à gauche M est dit **libre** si $M = \{0\}$ ou si M a une base. Si $\mathcal{B}$ est une base de M, on dit que M est **libre sur** $\mathcal{B}$.

Similairement, on définit la base d'un R-module à droite.

Comme pour les espaces vectoriels, on peut facilement voir que la représentation d'un vecteur v dans un R-module (à gauche ou à droite) libre sur une base $\mathcal{B}$ est essentiellement unique (c'est-à-dire unique modulo une permutation de l'ordre des termes dans une combinaison linéaire des vecteurs de base).

De plus, toujours de manière similaire au cas des espaces vectoriels, on peut définir un opérateur linéaire sur un R-module (à gauche ou à droite) libre simplement en assignant une valeur arbitraire à chaque élément d'une base. En effet, si M et N sont deux R-modules (disons à gauche) où M est libre sur la base $\mathcal{B} = \{b_i \mid i \in I\}$. Alors on peut définir un unique R-opérateur $\tau : M \to N$ en spécifiant les valeurs des τb_i arbitrairement pour

tous les $b_i \in \mathcal{B}$ et en étendant τ sur M par linéarité, *i.e.* pour tout $a_1, \ldots, a_n$ dans R et $i_1, \ldots, i_n$ dans I

$$\tau(a_1 b_{i_1} + \cdots + a_n b_{i_n}) = a_1 \tau b_{i_1} + \cdots + a_n \tau b_{i_n}.$$

Module sur un Corps Gauche

Une condition suffisante pour qu'un module (à gauche ou à droite) de génération finie soit libre est que son anneau de base soit un corps gauche. Nous allons le voir avec le lemme suivant.

1.11 Lemme de dépendance linéaire. Soit M un module (à gauche ou à droite) de génération finie sur un corps gauche D. Si la liste $(v_1, \ldots, v_m)$ d'éléments de M est linéairement dépendante et si $v_1 \neq 0$, alors il existe $j \in \{2, \ldots, m\}$ tel que

(a) $v_j \in \text{span}(v_1, \ldots, v_{j-1})$;

(b) on peut enlever le j$^{\text{ème}}$ terme de la liste $(v_1, \ldots, v_m)$ sans changer le span de la liste.

PREUVE. (*tirée de [1, p. 25])* Nous construisons la preuve dans la cas d'un module *à gauche*. Comme la liste $(v_1, \ldots, v_m)$ est linéairement dépendante, il existe des scalaires $a_1, \ldots, a_n \in D$ pas tous zéro dans R tels que

$$a_1 v_1 + \cdots + a_n v_n = 0.$$

Comme le module est sur un corps gauche, si $a_1 v_1 = 0$ et $a_1 \neq 0$, on a $v_1 = 1 v_1 = a_1^{-1} a_1 v_1 = 0$, ce qui contredit notre hypothèse sur v_1. On a donc forcément qu'au moins un facteur parmi $a_2, \ldots, a_n$ n'est pas zéro.

Soit $j \in \{2, \ldots, n\}$ l'indice maximal tel que $a_j \neq 0$. Ainsi,

$$v_j = a_j^{-1} a_1 v_1 + \cdots + a_j^{-1} a_{j-1} v_{j-1}, \tag{1.12}$$

ce qui montre la première partie.

Pour voir (b), supposons que $u \in \text{span}(v_1, \ldots, v_n)$. Alors, il existe des scalaires $b_1, \ldots, b_n$ tels que

$$u = b_1 v_1 + \cdots + b_n v_n.$$

Dans cette équation, nous pouvons remplacer v_j par son expression dans (1.12), ce qui montre que le span de la liste privée de v_j reste inchangé. □

Le lemme montre qu'on peut toujours construire une base dans un module (à gauche ou à droite) de génération finie sur un corps gauche : on part

d'une liste de vecteurs engendrant le module, puis en utilisant le lemme successivement, on obtient une suite de listes engendrant le module de longueur décroissante. Le processus s'arrête quand on trouve une liste linéairement indépendante, qui est alors une base du module.

On a ainsi le corollaire :

1.13 Corollaire. Tout module (à gauche ou à droite) de génération finie sur un corps gauche est libre.

Une deuxième propriété intéressante d'un module de génération finie sur un corps gauche est que toutes ses bases ont la même longueur. Pour le voir, il nous faut le théorème suivant.

1.14 Théorème. Si M est un module (à gauche ou à droite) de génération finie sur un corps gauche D, alors la longueur de chaque liste finie de vecteurs engendrant M est au moins la longueur de chaque liste finie de vecteurs linéairement indépendants.

PREUVE. (*tirée de [1, p. 25-26]*) Soit $(u_1, \ldots, u_m)$ une liste de vecteurs de M linéairement indépendants et soit $(w_1, \ldots, w_n)$ une liste engendrant M. Il nous faut voir que $m \leq n$. Nous allons le faire à travers le processus suivant :

Étape 1

La liste $(w_1, \ldots, w_n)$ engendre M ; ainsi, lui adjoindre un vecteur produit une liste linéairement dépendante. En particulier, la liste

$$(u_1, w_1, \ldots, w_n)$$

est linéairement dépendante. Ainsi, par le lemme de dépendance linéaire, on peut enlever un w_i de cette liste sans changer son span. On obtient une nouvelle liste B de longueur n contenant u_1 et engendrant M.

Étape j

La liste B de l'étape $j-1$ engendre M ; ainsi, lui adjoindre un vecteur produit une liste linéairement dépendante. En particulier, la liste de longueur $(n+1)$ obtenue en ajoutant u_j à B (en le plaçant juste après $u_1, \ldots, u_{j-1}$) est linéairement dépendante. Par le lemme de dépendance linéaire, un des vecteurs de la nouvelle liste est alors dans le span des précédents, et, comme $(u_1, \ldots, u_j)$ est linéairement indépendante par hypothèse, ce vecteur doit être l'un des w_i. On peut donc enlever un des w_i de la liste B pour obtenir une nouvelle liste B (de longueur n), contenant $u_1, \ldots, u_j$ et le reste des w_i, et qui engendre toujours M.

Après m étapes, nous avons ajouté tous les u_i à la liste et le processus s'arrête. Si, à n'importe quelle étape, nous n'avions plus eu de w_i à enlever de la liste, alors nous aurions obtenu une contradiction. Ainsi, il doit y avoir au moins autant de w_i que de u_i. □

On remarque que si, dans le théorème, la liste $(u_i) \subseteq M$ de vecteurs linéairement indépendants avait été de taille infinie, alors un raisonnement similaire à celui du théorème aurait produit une contradiction. Ainsi, dans M, toute liste de vecteurs linéairement indépendants est finie.

Du théorème, on déduit que toutes les bases d'un module M (à gauche ou à droite) de génération finie sur un corps gauche ont même longueur. En effet, si B_1 et B_2 sont deux bases de M, alors chaque liste est linéairement indépendante et donc de longueur finie. Ainsi on peut leur appliquer le théorème : en considérant que B_1 est linéairement indépendante et que B_2 engendre M, on a que la longueur de B_1 est inférieure à celle de B_2 ; en échangeant les rôles de B_1 et de B_2, on obtient l'inégalité inverse et on peut conclure. Ceci nous permet de définir la dimension d'un module (à gauche ou à droite) de génération finie sur un corps gauche.

1.15 Définition. La **dimension** d'un module (à gauche ou à droite) de génération finie sur un corps gauche est la longueur d'une base du module.

Algèbre de Hamilton

L'**algèbre de Hamilton** $\mathbb{H}$ est un exemple célèbre de corps gauche. L'ensemble $\mathbb{H}$, dont les éléments sont appelés **quaternions**, est le sous-espace de $\mathbb{M}_2(\mathbb{C})$ (vu comme $\mathbb{R}$-espace vectoriel) engendré par la base

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$
$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ainsi,

$$\mathbb{H} := \operatorname{span}(1, i, j, k) = \left\{ \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\}.$$

On constate que $\mathbb{H}$ est clos par multiplication. En effet, pour tout $a, b, c, d \in \mathbb{C}$, on a

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{b}c - \overline{ad} & -d\overline{b} + \overline{ac} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{ad + b\overline{c}} & \overline{ac - b\overline{d}} \end{pmatrix}.$$

De plus, tous les éléments non-nuls de $\mathbb{H}$ ont un inverse multiplicatif dans $\mathbb{H}$. En effet, pour $a, b \in \mathbb{C}$, on a

$$\Delta = \det \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = |a|^2 + |b|^2$$

qui est toujours strictement positif si la matrice est non-nulle ; l'inverse s'écrit explicitement comme

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}^{-1} = \frac{1}{\Delta} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} = \frac{1}{\Delta} \begin{pmatrix} \overline{a} & -b \\ -\overline{-b} & \overline{\overline{a}} \end{pmatrix}$$

qui a la forme des éléments de $\mathbb{H}$ décrite ci-avant.

Ainsi, si on munit $\mathbb{H}$ de l'addition, de la multiplication scalaire et de la multiplication standards de $\mathbb{M}_2(\mathbb{C})$ (vu comme un $\mathbb{R}$-espace vectoriel), $\mathbb{H}$ devient un corps gauche ; et, comme tout corps gauche est simple, il est, avec cette structure, simple.

Comme les éléments de $\mathbb{H}$ s'écrivent tous comme une combinaison linéaire d'éléments de la base $\{1, i, j, k\}$, la multiplication sur $\mathbb{H}$ est entièrement déterminée par la table suivante :

(a) $1x = x1 = x$ pour tout $x \in \{1, i, j, k\}$,

(b) $i^2 = j^2 = k^2 = -1$,

(c) $ij = k$, $jk = i$, $ki = j$,

(d) $ji = -k$, $kj = -i$, $ik = -j$.

Une inspection de cette table nous apprend que $\mathbb{H}$ n'est pas commutatif, comme, par exemple, $ik = -ki$.

Pour décrire le centre de $\mathbb{H}$, prenons $a + bi + cj + dk \in \mathcal{Z}(\mathbb{H})$, qui doit, en particulier, commuter avec tous les éléments de la base $\{1, i, j, k\}$. On pose la condition sur i :

$$i(a + bi + cj + dk) = (a + bi + cj + dk)i.$$

On trouve, en utilisant la table, $c = d = 0$, et en réécrivant la condition avec j, on conclut que le centre de $\mathbb{H}$ est réduit à la copie de $\mathbb{R}$ dans $\mathbb{H}$

$$\mathcal{Z}(\mathbb{H}) = \mathbb{R}1.$$

Le corps-gauche $\mathbb{H}$ est donc $\mathbb{R}$-central.

Notons pour finir que l'on peut assimiler $\mathbb{H}$ à $\mathbb{R}^4$ comme $\mathbb{H}$ est un $\mathbb{R}$-espace vectoriel de dimension 4.

1.16 Remarque. On verra, dans le chaptitre 4, une définition plus générale des quaternions.

Algèbre des Matrices sur un Corps Gauche

1.17 Notations. Soit R un anneau unitaire et $n \geq 1$. On définit la matrice $E_{ij} \in \mathbb{M}_n(R)$ pour $i, j = 1, \ldots, n$ par

$$(E_{ij})_{ij} = 1 \quad \text{et} \quad (E_{ij})_{kl} = 0, \text{ pour tout } (k,l) \neq (i,j).$$

On définit aussi la matrice $E_i \in \mathbb{M}_n(R)$ pour $i = 1, \ldots, n$ par

$$E_i = E_{ii}.$$

1.18 Propriétés. Soit $A \in \mathbb{M}_n(R)$ (avec $n \geq 1$) une matrice construite sur un anneau unitaire R. On a alors

(a) pour $i, j = 1, \ldots, n$

$$(E_i \cdot A)_{kl} = \begin{cases} A_{kl} & \text{si } k = i, \\ 0 & \text{sinon,} \end{cases}$$

$$\text{et} \quad (A \cdot E_j)_{kl} = \begin{cases} A_{kl} & \text{si } l = j, \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, multiplier à *gauche* par E_i revient à sélectionner la $i^{\text{ème}}$ *ligne*, et multiplier à *droite* par E_j revient à sélectionner la $j^{\text{ème}}$ *colonne*.

(b) pour $a, b, c = 1, \ldots, n$

$$E_{ab} \cdot E_{bc} = E_{ac}.$$

PREUVE. La vérification est une routine. □

1.19 Proposition. Soit D un corps gauche sur un corps F. La F-algèbre $\mathbb{M}_n(D)$ est simple pour tout $n \geq 1$.

PREUVE. Soit $A \in \mathbb{M}_n(D)$. Avec les notations de (1.17) et la partie (a) de (1.18), on a que pour $i, j = 1, \ldots, n$

$$(E_i \cdot A \cdot E_j)_{kl} = \begin{cases} A_{kl} & \text{si } (k,l) = (i,j), \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, si $A_{ij} \neq 0$,

$$(A_{ij}^{-1} \mathbb{1}_n) \cdot (E_i \cdot A \cdot E_j) = E_{ij} \tag{1.20}$$

Soit I un idéal bilatère non-zéro de $\mathbb{M}_n(D)$. Il existe $A \in I$ avec un couple d'indices i, j tels que $A_{ij} \neq 0$. En utilisant (1.20), on a que $E_{ij} \in I$. De ceci (et en utilisant la partie (b) de (1.18)) on déduit que $E_{kl} \in I$ pour tout couple k, l d'indices.

Ainsi, I contient la base de $\mathbb{M}_n(D)$ (vu comme D-module)

$$\{E_{kl} \mid k, l \in \{1, \dots n\}\}.$$

De plus, I est stable par multiplication "scalaire" par un élément de D comme, pour $M \in I$ et $\lambda \in D$,

$$(\lambda \mathbb{1}_n)M \in I\,;$$

on note enfin que I est stable par addition (car I est un sous-groupe de $\mathbb{M}_n(D)$). On peut donc conclure que $I = M$, comme voulu. □

1.21 Proposition. Soit D un corps gauche sur un corps F, et $n \geq 1$. Alors

(a) l'inclusion

$$\Phi : \mathcal{Z}(D) \longrightarrow \mathcal{Z}(\mathbb{M}_n(D)), \quad x \longmapsto x\mathbb{1}_n,$$

est surjective ;

(b) si D est F-central, alors $\mathbb{M}_n(D)$ est aussi F-central.

Preuve. *Partie* (a) : Il est clair que

$$\{\lambda \mathbb{1}_n \mid \lambda \in \mathcal{Z}(D)\} \subseteq \mathcal{Z}(\mathbb{M}_n(D)). \tag{1.22}$$

Si nous montrons qu'il y a égalité dans (1.22), alors nous aurons que Φ est surjective.

Choisissons une matrice $m \in \mathcal{Z}(\mathbb{M}_n(D))$ quelconque et essayons de trouver des conditions sur sa forme.

Premièrement, il faut que m commute avec tous les E_i définis en (1.17), or l'équation $E_i \cdot m = m \cdot E_i$ se traduit par

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ m_{i1} & m_{i2} & \cdots & m_{in} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & \cdots & m_{1i} & \cdots & 0 \\ 0 & \cdots & m_{2i} & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & m_{ni} & \cdots & 0 \end{pmatrix}.$$

Ainsi m est une matrice diagonale.

Notons par z la matrice de $\mathbb{M}_n(D)$ composée uniquement de 1, *i.e.* $(z)_{ij} = 1$ pour tout $i, j = 1, \ldots, n$. On doit avoir $z \cdot m = m \cdot z$, c'est-à-dire

$$\begin{pmatrix} m_{11} & m_{22} & \cdots & m_{nn} \\ m_{11} & m_{22} & \cdots & m_{nn} \\ \vdots & \vdots & & \vdots \\ m_{11} & m_{22} & \cdots & m_{nn} \end{pmatrix} = \begin{pmatrix} m_{11} & m_{11} & \ldots & m_{11} \\ m_{22} & m_{22} & \ldots & m_{22} \\ \vdots & \vdots & & \vdots \\ m_{nn} & m_{nn} & \ldots & m_{nn} \end{pmatrix}.$$

Ainsi, tous les m_{ii} sont égaux, *i.e.* m est de la forme $\lambda \mathbb{1}_n$ pour un certain $\lambda \in D$. Nous voulons pouvoir restreindre λ à $\mathcal{Z}(D)$.

Si $\lambda \notin \mathcal{Z}(D)$, alors il existe $\mu \in D$ tel que $\lambda\mu \neq \mu\lambda$, et on a $m \cdot (\mu \mathbb{1}_n) \neq (\mu \mathbb{1}_n) \cdot m$, ce qui contredit $m \in \mathcal{Z}(\mathbb{M}_n(D))$. Ainsi $\lambda \in \mathcal{Z}(D)$, ce qui finit de montrer qu'il y a égalité dans (1.22). On conclut que Φ est surjective.

Partie (b) : Si D est F-central, alors par (a)

$$\mathcal{Z}(\mathbb{M}_n(D)) = \Phi(\mathcal{Z}(D)) = \Phi(F1) = (F1)\mathbb{1}_n = F\mathbb{1}_n \ ;$$

le centre de $\mathbb{M}_n(D)$ est donc réduit à la copie de F dans $\mathbb{M}_n(D)$, on ainsi que $\mathbb{M}_n(D)$ est F-centrale, comme voulu. □

Lemme de Schur

1.23 Définition. Soient A une algèbre sur un corps F et M un A-module à gauche. On dit que M est **simple** si $\{0\}$ et M sont les seuls A-sous-modules à gauche de M.

1.24 Proposition. Soient A une algèbre sur un corps F, M_1, M_2 deux A-modules à gauche et $\varphi : M_1 \longrightarrow M_2$ un homomorphisme de A-modules. Alors

(a) $\varphi(M_1)$ est un A-sous-module de M_2 ;

(b) Si M_1 et M_2 sont simples et que $\varphi \neq 0$, alors φ est bijective.

Preuve. La partie (a) découle de φ homomorphisme de A-modules. Pour la partie (b), on commence par remarquer que φ est surjective ; en effet, le point (a) implique que

$$\varphi(M_1) = \{0\} \text{ ou } M_2,$$

et on a supposé que $\varphi \neq 0$. Pour voir l'injectivité de φ on suppose qu'il existe $x \in M_1 \setminus \{0\}$ tel que $\varphi(x) = 0$. Comme Ax est un A-sous module de M_1 et que M_1 est simple, on a $Ax = M_1$. Ainsi

$$\varphi(M_1) = \varphi(Ax) = A\varphi(x) = \{0\} \ ;$$

ce qui contredit $\varphi \neq 0$. On a donc $\mathrm{Ker}(\varphi) = \{0\}$, *i.e.* φ est injective. □

1.25 Définition. Soient A une algèbre sur un corps F et M un A-module à gauche. On note

$$\mathrm{End}_A(M) := \{\varphi : M \to M \mid \varphi \text{ endomorphisme de } A\text{-modules à gauche}\}.$$

l'ensemble des endomorphismes de A-modules à gauche sur M. On munit cet ensemble d'une structure de F-algèbre en définissant, pour tout $\varphi, \psi \in \mathrm{End}_A(M)$, $m \in M$ et $\lambda \in F$, l'addition par

$$(\varphi + \psi)(m) := \varphi(m) + \psi(m),$$

la multiplication par

$$(\varphi \circ \psi)(m) := \varphi(\psi(m)),$$

et la multiplication scalaire par

$$(\lambda\varphi)(v) := \lambda(\varphi(v)).$$

1.26 Lemme de Schur. Soient A une algèbre sur un corps F et M un A-module à gauche simple. Alors $\mathrm{End}_A(M)$ est un corps gauche.

Preuve. On applique la partie (b) de (1.24). □

1.27 Proposition. Soit D un corps gauche sur un corps F et $A = \mathbb{M}_n(D)$ ($n \geq 1$) l'anneau des matrices $n \times n$ construit sur D. On définit, pour $k \in \{1, \ldots, n\}$,

$$L_k := \{(a_{ij})_{i,j=1,\ldots,n} \in A \mid a_{ij} = 0 \text{ pour tout } j \neq k\} \subseteq A.$$

Alors

(a) L_k est un A-module à gauche simple ;

(b) Si M est un A-module à gauche simple non-zéro, alors M est isomorphe à L_l pour un $l \in \{1, \ldots, n\}$.

Preuve. *Partie* (a) : On peut vérifier que L_k est un idéal à gauche de A, L_k est donc un A-module à gauche. Pour voir que L_k est simple, choisissons un élément non-zéro z d'un A-sous-module à gauche non-zéro L' de L_k. On a qu'il existe un indice i tel que $z_{ik} \neq 0$; et ainsi, en utilisant les notations de (1.17) et la partie (a) de (1.18),

$$(z_{ik}^{-1}\mathbb{1}_n) \cdot E_i \cdot z = E_{ik};$$

d'où $E_{ik} \in L'$, et comme en sait (partie (b) de (1.18)) que pour tout $a \in \{1, \ldots, n\}$

$$E_{ai} \cdot E_{ik} = E_{ak},$$

on a que la base de L_k

$$\{E_{ak} \mid a \in \{1, \ldots, n\}\}$$

est dans L', *i.e.* $L' = L_k$.

Partie (b) : On remarque que $A = \sum_{k=1}^{n} L_k$ et que $\{0\} \neq M = AM$, ainsi

$$\{0\} \neq AM = \left(\sum_{k=1}^{n} L_k\right) M = \sum_{k=1}^{n} (L_k M).$$

Il existe donc un indice l tel que $L_l M \neq \{0\}$. On peut ainsi trouver un couple (l, m) avec l un indice et $m \in M$ tels que $L_l m \neq \{0\}$. On définit l'homomorphisme de A-modules de multiplication à droite par m

$$r_m : L_l \longrightarrow M, \quad x \longmapsto xm \ ;$$

par la partie (b) de (1.24), on a que r_m est un isomorphisme. □

Algèbres Opposées

1.28 Définition. Soit $(A, +, \cdot)$ une algèbre sur un corps F. On définit son **algèbre opposée** $(A^{\mathrm{op}}, +, \cdot_{\mathrm{op}})$ par

$$(A^{\mathrm{op}}, +) := (A, +),$$

et par

$$a \cdot_{\mathrm{op}} b := b \cdot a \quad \text{pour tout } a, b \in A^{\mathrm{op}}.$$

1.29 Proposition. Soit F un corps. Soit M un module à gauche sur un F-corps gauche D, tel que $\dim_D(M) = n < \infty$. Alors on a l'isomorphisme de F-algèbres

$$\mathrm{End}_D(M) \cong \mathbb{M}_n(D^{\mathrm{op}}).$$

Preuve. Soit $\mathcal{B} = \{m_1, \ldots, m_n\} \subseteq M$ une base de M. On définit un isomorphisme (de D-modules à gauche) qui associe à tout vecteur de M ses composantes dans $\mathcal{B}$

$$\begin{array}{rccc} [\,.\,]_{\mathcal{B}} : & M & \longrightarrow & D^n \\ & \sum_{k=1}^{n} x_k m_k & \longmapsto & [x]_{\mathcal{B}} = (x_1, \ldots, x_k). \end{array}$$

On peut alors définir

$$\begin{array}{rccc} \Psi: & \mathrm{End}_D(M) & \longrightarrow & \mathbb{M}_n(D^{\mathrm{op}}) \\ & \varphi & \longmapsto & (\Psi(\varphi))_{ij} = \big([\varphi(m_j)]_{\mathcal{B}}\big)_i\,. \end{array}$$

Comme le choix des images dans M des éléments d'une base de M permet de définir un endomorphisme (de D-module à gauche) de M, et ce de manière unique, on a la bijectivité de Ψ.

Comme $[\ .\ ]_{\mathcal{B}}$ et $(\ .\ )_i$ (pour $i = 1, \ldots, n$) sont deux homomorphismes de D-modules, on déduit que Ψ est additive et F-homogène.

On constate encore que $\Psi(\mathrm{Id}_M) = \mathbb{1}_n$. Il nous reste à voir que, pour φ, ξ dans $\mathrm{End}_D(M)$, on a

$$\Psi(\varphi \circ \xi) = \Psi(\varphi) \cdot \Psi(\xi) \tag{1.30}$$

pour pouvoir conclure que Ψ est bien un isomorphisme de F-algèbres.

Écrivons pour $i = 1, \ldots, n$

$$\begin{aligned} \varphi(m_j) &= \sum_{k=1}^{n} a_{kj} m_k, \qquad \text{et} \\ \xi(m_j) &= \sum_{k=1}^{n} b_{kj} m_k. \end{aligned}$$

Ainsi

$$\begin{aligned} (\Psi(\varphi))_{ij} &= ([\varphi(m_j)]_{\mathcal{B}})_i = a_{ij}, \qquad \text{et} \\ (\Psi(\xi))_{ij} &= ([\xi(m_j)]_{\mathcal{B}})_i = b_{ij}. \end{aligned}$$

En utilisant ces deux dernières équations, on a

$$\begin{aligned} (\Psi(\varphi) \cdot \Psi(\xi))_{ij} &= \sum_{k=1}^{n} (\Psi(\varphi))_{ik} \cdot_{\mathrm{op}} (\Psi(\xi))_{kj} \\ &= \sum_{k=1}^{n} a_{ik} \cdot_{\mathrm{op}} b_{kj} = \sum_{k=1}^{n} b_{kj} a_{ik}. \end{aligned} \tag{1.31}$$

On calcule

$$(\varphi \circ \xi)(m_j) = \varphi\left(\sum_{k=1}^{n} b_{kj} m_k\right) = \sum_{\substack{k=1,\ldots,n \\ l=1,\ldots,n}} b_{kj} a_{lk} m_l,$$

ainsi

$$(\Psi(\varphi\circ\xi))_{ij} = \big([(\varphi\circ\xi)(m_j)]_{\mathcal{B}}\big)_i = \sum_{k=1}^{n} b_{kj}a_{ik}. \tag{1.32}$$

De (1.31) et (1.32), on conclut à (1.30), comme voulu. □

1.33 Proposition. Soit D un corps gauche sur un corps F, et soit $n \geq 1$. On note $A := \mathbb{M}_n(D)$. Alors

(a) le A-module à gauche

$$D^n = \left\{ \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \;\middle|\; d_1, \ldots, d_n \in D \right\}$$

est simple ;

(b) il existe un isomorphisme de F-algèbres

$$D^{\mathrm{op}} \cong \mathrm{End}_A(D^n).$$

Preuve. *Partie* (a) : Soit $k \in \{1, \ldots, n\}$. Il est clair, avec les notations de (1.27), que $L_k \cong D^n$ en tant que A-modules à gauche. Ainsi, comme par la partie (a) de (1.27), L_k est simple, on a que D^n est simple.

Partie (b) : À tout $d \in D^{\mathrm{op}}$, on associe l'endomorphisme de A-modules à gauche de multiplication à droite

$$r_d : D^n \longrightarrow D^n, \quad \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \longmapsto \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} d := \begin{pmatrix} d_1 d \\ \vdots \\ d_n d \end{pmatrix}.$$

Nous allons voir que

$$\Phi : D^{\mathrm{op}} \longrightarrow \mathrm{End}_A(D^n), \quad d \longmapsto r_d$$

est l'isomorphisme de F-algèbres que nous cherchons.

(i) Φ *homomorphisme de F-algèbres* : soit $e, d \in D^{\mathrm{op}}$, $\lambda \in F$ et $x \in D^n$.

On calcule

$$\begin{aligned}\Phi(d+e)(x) &= r_{d+e}(x) = x(d+e) = xd + xe = r_d(x) + r_e(x)\\ &= (r_d + r_e)(x) = (\Phi(d) + \Phi(e))(x),\\ \Phi(\lambda d)(x) &= r_{\lambda d}(x) = x(\lambda d) = \lambda(xd) = \lambda(r_d(x))\\ &= (\lambda r_d)(x) = (\lambda\Phi(d))(x),\\ \Phi(d \cdot_{\mathrm{op}} e)(x) &= r_{d\cdot_{\mathrm{op}} e}(x) = x(d \cdot_{\mathrm{op}} e) = x(ed) = (xe)d = r_d(xe)\\ &= r_d(r_e(x)) = (r_d \circ r_e)(x) = (\Phi(d) \circ \Phi(e))(x).\end{aligned}$$

(ii) Φ *injective* : comme $\Phi(1) = \mathrm{Id}_{D^n} \neq 0$, on a $\Phi \neq 0$. Or D^{op} est une F-algèbre simple (comme un corps gauche est toujours simple). Ainsi,

$$\mathrm{Ker}(\Phi) = D^{\mathrm{op}} \text{ ou } \{0\},$$

et comme on vient de voir que $\Phi \neq 0$, on a $\mathrm{Ker}(\Phi) = \{0\}$, *i.e.* Φ est injective.

(iii) Φ *surjective* : soit $\{e_1, \ldots, e_n\}$ la base standard de D^n en tant que D-module et soit $f \in \mathrm{End}_A(D^n)$ quelconque. On remarque que pour tout $d \in D$ et $x \in D^n$, on a

$$f(dx) = f((d\mathbb{1}_n)x) = (d\mathbb{1}_n)f(x) = df(x),$$

i.e. f est aussi un endomorphisme de D-modules à gauche.
On peut trouver des scalaires $d_1, \ldots, d_n \in D$ tels que

$$f(e_1) = e_1 d_1 + \cdots + e_n d_n.$$

Ainsi, en utilisant les E_{ij} définis en (1.17), on a que pour tout vecteur $v = \sum_{i=1}^n \lambda_i e_i \in D^n$ avec $\lambda_1, \ldots, \lambda_n \in D$

$$\begin{aligned}f(v) &= \sum_{i=1}^n \lambda_i f(e_i) = \sum_{i=1}^n \lambda_i f(E_{i1}e_1) = \sum_{i=1}^n \lambda_i E_{i1} f(e_1)\\ &= \sum_{i=1}^n \lambda_i E_{i1}(e_1 d_1 + \cdots + e_n d_n).\end{aligned}$$

Or $E_{i1}e_1 = e_i$, et pour tout $j \neq 1$, $E_{i1}e_j = 0$, ainsi

$$f(v) = \sum_{i=1}^n \lambda_i e_i d_1 = r_{d_1}(v).$$

On a donc $f \in \Phi(D^{\mathrm{op}})$, *i.e.* Φ est surjective.

□

Lemme de Rieffel

Si A est une algèbre sur un corps F et si M est un A-module à gauche, alors on peut équiper M d'une structure de module à gauche sur l'anneau de base $E := \mathrm{End}_A(M)$ en définissant la multiplication scalaire par

$$\varphi \cdot m := \varphi(m), \quad \text{pour } \varphi \in \mathrm{End}_A(M) \text{ et } m \in M.$$

1.34 Lemme. Soit A une algèbre sur un corps F et M un A-module à gauche. Alors la **multiplication à gauche** définie pour $a \in A$ par

$$l_a : M \longrightarrow M, \quad m \longmapsto am$$

est un endomorphisme de E-modules à gauche.

Preuve. Soit $m, n \in M$ et $\varphi \in \mathrm{End}_A(M)$. On calcule

$$\begin{aligned} l_a(m+n) &= a(m+n) = am + an = l_a(m) + l_a(n), \\ l_a(\varphi \cdot m) &= a(\varphi \cdot m) = a(\varphi(m)) = \varphi(am) = \varphi \cdot (am) = \varphi \cdot l_a(m). \end{aligned}$$

□

1.35 Lemme. Soit A une algèbre sur un corps F et M un A-module à gauche. Alors l'application

$$\lambda_M : A \longrightarrow \mathrm{End}_E(M), \quad a \longmapsto l_a$$

est un homomorphisme de F-algèbres.

Preuve. Soit $a, b \in A$, $m \in M$ et $\mu \in F$. On calcule

$$\begin{aligned} \lambda_M(a+b)(m) &= l_{a+b}(m) = (a+b)m = am + bm \\ &= (l_a + l_b)(m) = (\lambda_M(a) + \lambda_M(b))(m), \\ \lambda_M(\mu a)(m) &= l_{\mu a}(m) = (\mu a)m = \mu(am) = \mu l_a(m) = (\mu \lambda_M(a))(m), \\ \lambda_M(ab)(m) &= l_{ab}(m) = (ab)m = a(l_b(m)) = l_a(l_b(m)) \\ &= (l_a \circ l_b)(m) = (\lambda_M(a) \circ \lambda_M(b))(m). \end{aligned}$$

□

1.36 Lemme de Rieffel. Soit A une algèbre *simple* sur un corps F et L un idéal à gauche de A non-zéro. En écrivant $E := \mathrm{End}_A(L)$ et en définissant λ_L similairement à (1.35) par

$$\lambda_L : A \longrightarrow \mathrm{End}_E(L), \quad a \longmapsto l_a$$

avec

$$l_a : L \longrightarrow L, \quad x \longmapsto ax,$$

alors on a que λ_L est un isomorphisme de F-algèbres.

PREUVE. *Injectivité* : le noyau de l'homomorphisme de F-algèbres λ_L est un idéal bilatère de A, ainsi

$$\mathrm{Ker}(\lambda_L) = \{0\} \text{ ou } A,$$

il nous suffit donc de voir que $\lambda_L \neq 0$ pour avoir son injectivité. On remarque que $\lambda_L(1) = l_1 = \mathrm{Id}_L \neq 0$, comme $L \neq (0)$.

Surjectivité : soit $x \in L$ quelconque. On commence par définir l'endormophisme de A-module à gauche de **multiplication à droite**

$$r_x : L \longrightarrow L \quad y \longmapsto yx.$$

On a $r_x \in E$. On va utiliser ce fait pour voir que $\lambda_L(L)$ est un idéal à gauche de $\mathrm{End}_E(L)$. Comme nous savons déjà que $\lambda_L(L)$ est un sous-groupe de $\mathrm{End}_E(L)$ comme il est l'image d'un groupe par un homomorphisme de F-algèbres, il nous suffit de voir qu'il est stable par multiplication à gauche par les éléments de $\mathrm{End}_E(L)$, *i.e.* on choisit $\varphi \in \mathrm{End}_E(L)$ et $l \in L$ et on veut montrer que $\varphi \circ \lambda_L(l) \in \lambda_L(L)$. Soit $x \in L$, on calcule

$$\begin{aligned}(\varphi \circ \lambda_L(l))(x) = \varphi(\lambda_L(l)(x)) = \varphi(lx) = \varphi(r_x \cdot l)\\ = r_x \cdot \varphi(l) = \varphi(l)x = \lambda_L(\varphi(l))(x),\end{aligned}$$

ainsi $\varphi \circ \lambda_L(l) = \lambda_L(\varphi(l)) \in \lambda_L(L)$, d'où $\lambda_L(L)$ idéal à gauche de $\mathrm{End}_E(L)$.

Comme

$$LA := \left\{ \sum_{i=1}^{n} l_i a_i \;\middle|\; n \geq 1 \text{ et } (l_i, a_i) \in L \times A \text{ pour } i = 1, \ldots, n \right\}$$

est un idéal bilatère non-zéro de A, on a $LA = A$ (comme A est simple). Ainsi, il est possible d'écrire $1 = \sum_{i=1}^{n} l_i a_i$, pour un certain entier $n \geq 1$ et une liste de couples $(l_i, a_i)_{i=1,\ldots,n} \subseteq L \times A$. Soit maintenant $\varphi \in \mathrm{End}_E(L)$ quelconque, on a que pour tout $x \in L$

$$\begin{aligned}\varphi(x) = \varphi(1x) = \sum_{i=1}^{n} \varphi(l_i a_i x) = \sum_{i=1}^{n} \varphi((\lambda_L(l_i) \circ \lambda_L(a_i))(x))\\ = \sum_{i=1}^{n} (\underbrace{\varphi \circ \lambda_L(l_i)}_{\in \lambda_L(L)} \circ \lambda_L(a_i))(x),\end{aligned}$$

il existe donc une liste $(l'_i)_{i=1,\dots,n} \subseteq L$ telle que

$$\begin{aligned}\varphi(x) &= \sum_{i=1}^{n} (\lambda_L(l'_i) \circ \lambda_L(a_i))(x) = \sum_{i=1}^{n} (l'_i a_i x) \\ &= \left(\sum_{i=1}^{n} l'_i a_i \right) x = \lambda_L \left(\sum_{i=1}^{n} l'_i a_i \right) (x),\end{aligned}$$

et ainsi, $\varphi \in \lambda_L(LA) = \lambda_L(A)$, ce qui montre la surjectivité de λ_L. □

Théorème de Wedderburn

1.37 Lemme. Soit A une algèbre de dimension *finie* sur un corps F. Alors il existe un idéal à gauche $L \subseteq A$ minimal (non-zéro).

PREUVE. Si A n'a pas d'idéal à gauche propre, il n'y a rien à faire. En effet, A est un idéal à gauche de A.

Considérons l'autre cas, *i.e.* A possède un idéal à gauche propre L_1. Comme L_1 est, en particulier, un F-sous-espace vectoriel propre de A, on a $\dim_F(L_1) < \dim_F(A)$. Si L_1 ne contient aucun sous-idéal à gauche non-trivial de A, alors on s'arrête. Sinon, il existe un idéal à gauche L_2 de A avec

$$\{0\} \subset L_2 \subset L_1 \subset A,$$

où toutes les inclusions sont strictes, *i.e.*

$$0 < \dim_F(L_2) < \dim_F(L_1) < \dim_F(A)\ ;$$

ainsi, à chaque nouvelle étape, la dimension de l'idéal à gauche L_i diminue. Le processus va donc s'arrêter après un nombre d'étapes borné par $\dim_F(A)$, et on obtient alors un idéal à gauche de A minimal. □

1.38 Lemme. Soit A et B deux algèbres sur un corps F. S'il existe un isomorphisme de F-algèbres

$$\pi : A \longrightarrow B$$

et si L_A est un idéal à gauche de A. Alors $L_B := \pi(L_A)$ est un idéal à gauche de B et on a l'isomorphisme de F-algèbres

$$\mathrm{End}_A(L_A) \cong \mathrm{End}_B(L_B).$$

PREUVE. On définit

$$\begin{array}{rccc} \Psi : & \mathrm{End}_A(L_A) & \longrightarrow & \mathrm{End}_B(L_B) \\ & \varphi & \longmapsto & \Psi(\varphi) = \pi \circ \varphi \circ \pi^{-1}. \end{array}$$

On vérifie que Ψ est bien définie, *i.e.* que pour $\varphi \in \mathrm{End}_A(L_A)$, on a

$$\pi \circ \varphi \circ \pi^{-1} \in \mathrm{End}_B(L_B).$$

On vérifie de plus que Ψ est un homomorphisme de F-algèbres.

Pour voir que Ψ est injective, choisissons φ dans $\mathrm{End}_A(L_A)$ tel que $\Psi(\varphi) = 0$. Pour tout $x \in L_B$, on a

$$\pi(\varphi(\pi^{-1}(x))) = 0$$

et donc $\varphi(\pi^{-1}(x)) = 0$. Or $\pi^{-1}(L_B) = L_A$. Ainsi on a $\varphi = 0$.

Pour voir la surjectivité de Ψ, on remarque que si $\gamma \in \mathrm{End}_B(L_B)$, alors

$$\Psi(\pi^{-1} \circ \gamma \circ \pi) = \pi \circ \pi^{-1} \circ \gamma \circ \pi \circ \pi^{-1} = \gamma.$$

□

1.39 Lemme. Soit A une algèbre sur un corps F et M_1, M_2 deux A-modules à gauche.

Si M_1 et M_2 sont isomorphes en tant que A-modules à gauche, alors on a l'isomorphisme de F-algèbres suivant

$$\mathrm{End}_A(M_1) \cong \mathrm{End}_A(M_2).$$

PREUVE. On définit un isomorphisme Ψ de la même manière que dans la preuve de (1.38). □

1.40 Théorème de Wedderburn. Soit A une algèbre *simple* de dimension finie sur un corps F. Alors il existe un entier $n \geq 1$ et un corps gauche D sur F tels qu'il existe un isomorphisme de F-algèbres

$$A \cong \mathbb{M}_n(D).$$

De plus, n est unique et D est unique à isomorphisme de F-algèbres près.

PREUVE. *Existence* : On commence par appliquer le lemme (1.37) pour avoir un idéal à gauche $L \subseteq A$ minimal.

Comme A est une algèbre simple et que L est idéal à gauche non-trivial, on a par le lemme de Rieffel (1.36)

$$A \cong \mathrm{End}_{\mathrm{End}_A(L)}(L) \tag{1.41}$$

en tant que F-algèbres.

En tant que A-module à gauche, L ne peut par avoir de sous-A-module à gauche non-trivial, car cela contredirait sa minimalité. Ainsi L est un A-module à gauche simple. En appliquant le lemme de Schur (1.26), on a que $\mathrm{End}_A(L)$ est un corps gauche.

En notant n la dimension de L en tant que $\mathrm{End}_A(L)$-module, on a par la proposition (1.29)

$$\mathrm{End}_{\mathrm{End}_A(L)}(L) \cong \mathbb{M}_n(\mathrm{End}_A(L)^{\mathrm{op}}) \tag{1.42}$$

en tant que F-algèbres.

En combinant les équations (1.41) et (1.42), on a les isomorphismes de F-algèbres

$$A \cong \mathrm{End}_{\mathrm{End}_A}(L) \cong \mathbb{M}_n(\mathrm{End}_A(L)^{\mathrm{op}}).$$

et $\mathrm{End}_A(L)^{\mathrm{op}}$ est un corps gauche, comme nous avons vu ci-dessus que $\mathrm{End}_A(L)$ l'est.

Unicité : Soient $n, m \geq 1$ deux entiers et E, D deux corps gauches tels qu'on ait les isomorphismes de F-algèbres suivant

$$\mathbb{M}_n(D) \cong A \cong \mathbb{M}_m(E).$$

Soit $\pi : \mathbb{M}_n(D) \longrightarrow \mathbb{M}_m(E)$ un isomorphisme de F-algèbres. On choisit L_D un idéal minimal de $\mathbb{M}_n(D)$ (son existence est assurée par (1.37)).

On pose $L_E := \pi(L_D)$, qui est un idéal à gauche minimal de $\mathbb{M}_m(E)$. En effet, L_E est un idéal à gauche car c'est l'image par π d'un idéal à gauche et L_E est minimal car s'il existait un idéal à gauche non-trivial de $\mathbb{M}_m(E)$ contenu dans L_E, alors π^{-1} de cet idéal serait un idéal à gauche non-trivial de $\mathbb{M}_n(D)$ contenu dans L_D, ce qui contredirait la minimalité de L_D.

On va montrer les isomorphismes de F-algèbres suivant.

$$\begin{array}{ccc}
\mathrm{End}_{\mathbb{M}_n(D)}(L_D) & \cong & \mathrm{End}_{\mathbb{M}_m(E)}(L_E) \\
\wr\| & & \|\wr \\
\mathrm{End}_{\mathbb{M}_n(D)}(D^n) & & \mathrm{End}_{\mathbb{M}_m(E)}(E^m) \\
\wr\| & & \|\wr \\
D^{\mathrm{op}} & & E^{\mathrm{op}}
\end{array}$$

La première ligne découle de (1.38).

Pour avoir l'isomorphisme avec la deuxième ligne, on remarque que comme L_D est un $\mathbb{M}_n(D)$-module à gauche simple non-trivial, on a par la partie (b) de (1.27) que L_D est isomorphe à D^n en tant que $\mathbb{M}_n(D)$-module. Cela donne, en utilisant (1.39), l'isomorphisme de F-algèbres

$$\mathrm{End}_{\mathbb{M}_n(D)}(L_D) \cong \mathrm{End}_{\mathbb{M}_n(D)}(D^n).$$

On procède de même pour la partie de droite.

Pour avoir l'isomorphisme avec la troisième ligne, on applique la partie (b) de (1.33).

On déduit du diagramme l'isomorphisme de F-algèbres

$$E \cong D. \tag{1.43}$$

Il nous reste à voir que $n = m$. On va établir les isomorphismes de F-espaces vectoriels suivant.

$$\begin{array}{ccc} L_D & \cong & L_E \\ \wr\| & & \|\wr \\ D^n & & E^m \\ \wr\| & & \\ E^n & & \end{array}$$

Comme $L_E = \pi(L_D)$, on a que $L_E \cong L_D$ en tant que F-espaces vectoriels, d'où la première ligne.

On a vu plus haut que L_D est isomorphe à D^n en tant que $\mathbb{M}_n(D)$-module (et donc aussi en tant que F-espaces vectoriels), et comme par un raisonnement similaire, on a que L_E est isomorphe à E^m en tant que F-espaces vectoriels, on peut passer à la deuxième ligne.

Par (1.43), on a $E^n \cong D^n$ en tant que F-espaces vectoriels, d'où la troisième ligne.

On a donc l'isomorphisme de F-espaces vectoriels

$$E^n \cong E^m,$$

or ceci n'est possible que quand $m = n$. □

Chapitre 2

Produit Tensoriel

2.1 Définition. Soit V un espace vectoriel sur un corps F. On définit

$$F^V := \{f : V \to F \mid f(v) = 0 \text{ pour presque tout } v \in V\}.$$

On peut équiper F^V d'une structure d'espace vectoriel en définissant

$$(f + g)(v) := f(v) + g(v)$$

et

$$(\lambda f)(v) := \lambda f(v)$$

pour $f, g \in F^V$ et $\lambda \in F$.

Une base naturelle de F^V est $\{f_v \mid v \in V\}$ où f_v est défini par

$$f_v : \quad V \longrightarrow F, \quad w \longmapsto \begin{cases} 1 & \text{si } w = v, \\ 0 & \text{sinon.} \end{cases}$$

En effet, les f_v sont linéairement indépendants : s'il existe un sous-ensemble $I \subseteq V$ de cardinalité finie et des facteurs $(\lambda_v)_{v \in I} \subseteq F$ tels que $\sum_{v \in I} \lambda_v f_v = 0$, alors on a, pour tout $w \in I$, que $\left(\sum_{v \in I} \lambda_v f_v\right)(w) = 0$, *i.e.* $\lambda_w = 0$, d'où on conclut à l'indépendance linéaire.

Pour voir que les f_v engendrent F^V, on choisit un $f \in F^V$ quelconque. Par définition de F^V, il existe un ensemble $J \in V$ de cardinalité finie et des scalaires $(\mu_v)_{v \in J} \subseteq F$ tels que pour $w \in V$

$$f(w) = \begin{cases} \mu_w & \text{si } w \in J, \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, on peut écrire f comme une combinaison linéaire des f_v par

$$f = \sum_{v \in J} \mu_v f_v \ ; \tag{2.2}$$

les f_v engendrent donc F^V, ce qui finit de montrer qu'ils sont une base F^V.

Comme les deux ensembles V et $\{f_v \mid v \in V\}$ sont mis en bijection par l'application qui à $v \in V$ associe la fonction f_v de F^V correspondante, on écrira simplement v à la place de f_v par la suite.

2.3 Définition. Soient V et W deux espaces vectoriels sur un corps F, soit $R \subseteq F^{V \times W}$ le F-sous-espace vectoriel engendré par les éléments de la forme

$$\begin{array}{c} (\lambda v + \mu v', w) - \lambda(v, w) - \mu(v', w), \quad \text{et} \\ (v, \lambda w + \mu w') - \lambda(v, w) - \mu(v, w'), \end{array} \tag{2.4}$$

avec $v, v' \in V$, $w, w' \in W$ et $\lambda, \mu \in F$. On définit le **produit tensoriel** de V et de W comme

$$V \otimes_F W := F^{V \times W}/R.$$

On définit aussi

$$v \otimes w := (v, w) + R.$$

2.5 Propriétés. Soient V, W, F et R comme dans la définition. Pour $v, v' \in V$, $w, w' \in W$, $\lambda \in F$, on a

(a) $(v + v') \otimes w = v \otimes w + v' \otimes w$,

(b) $v \otimes (w + w') = v \otimes w + v \otimes w'$,

(c) $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$,

(d) l'élément neutre pour l'addition dans $V \otimes_F W$ est $(0, 0) + R$.

Preuve. Pour (a), on fait un calcul direct :

$$\begin{aligned} (v + v') \otimes w &= (v + v', w) + R \\ &= (v + v', w) - ((v + v', w) - (v, w) - (v', w)) + R \\ &= (v, w) + (v', w) + R \\ &= v \otimes w + v' \otimes w. \end{aligned}$$

La vérification de (b) est similaire à celle de (a).

Pour (c), on a que

$$\begin{aligned} \lambda(v \otimes w) &= \lambda((v, w) + R) = \lambda(v, w) + R \\ &= \lambda(v, w) + (\lambda v + 0 \cdot 0, w) - \lambda(v, w) - 0(0, w) + R \\ &= (\lambda v, w) + R, \end{aligned}$$

et on procède de même pour la deuxième égalité.

Pour (d), on commence par choisir $z + R \in V \otimes_F W$. Alors on a que

$$\begin{aligned}(z+R)+((0,0)+R) &= (z+(0,0))+R \\ &= (z+(0,0)+(0+0,0)-(0,0)-(0,0))+R \\ &= z+R.\end{aligned}$$

□

Soit $z \in V \otimes_F W$. On sait qu'il existe $z' \in F^{V\times W}$ tel que $z = z' + R$. En (2.2), on a vu qu'il existe une liste finie de couples $(v_i, w_i)_{i=1,\dots,n} \subseteq V \times W$ et des scalaires $(\lambda_i)_{i=1,\dots,n} \subseteq F$ tels que

$$z' = \sum_{i=1}^{n} \lambda_i (v_i, w_i).$$

Ainsi

$$\begin{aligned}z &= \left(\sum_{i=1}^{n} \lambda_i (v_i, w_i)\right) + R = \sum_{i=1}^{n} \lambda_i \left((v_i, w_i) + R\right) \\ &= \sum_{i=1}^{n} \lambda_i (v_i \otimes w_i) = \sum_{i=1}^{n} (\lambda_i v_i) \otimes w_i,\end{aligned}$$

et donc tout élément de $V \otimes_F W$ peut s'écrire comme une somme de produits tensoriels d'éléments de V et de W.

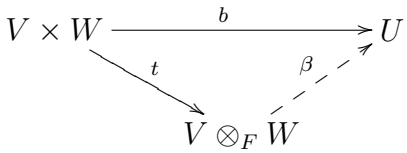
Propriété Universelle

2.6 Propriété universelle du produit tensoriel. Soient V, W et U trois espaces vectoriels sur un corps F. On définit

$$t : \quad V \times W \longrightarrow V \otimes_F W, \quad (v, w) \longmapsto v \otimes w.$$

et soit $b : V \times W \to U$ une forme bilinéaire.

Alors, il existe une unique forme linéaire $\beta : V \otimes_F W \to U$ avec $\beta(v \otimes w) = b(v, w)$, c'est-à-dire telle que le diagramme



commute.

PREUVE. L'unicité de β est immédiate, comme, pour tout $z \in V \otimes W$, on a vu qu'il existait un nombre fini de couples $(v_i, w_i)_{i=1,\dots,n} \subseteq V \times W$ tels que $z = \sum_{i=1}^{n} v_i \otimes w_i$, et donc

$$\beta(z) = \beta\left(\sum_{i=1}^{n} v_i \otimes w_i\right) = \sum_{i=1}^{n} \beta(v_i \otimes w_i) = \sum_{i=1}^{n} b(v_i, w_i),$$

qui est déterminé de manière unique.

Pour voir l'existence de β, commençons par définir une forme linéaire $b' : F^{V\times W} \to U$. Soit $x \in F^{V\times W}$, alors on sait qu'il existe une liste finie de couples $(v_i, w_i)_{i=1,\dots,n} \subseteq V \times W$ et des scalaires $(\lambda_i)_{i=1,\dots,n} \subseteq F$ tels que x s'écrit de manière unique comme $x = \sum_{i=1}^{n} \lambda_i(v_i, w_i)$. On pose

$$b'(x) := \sum_{i=1}^{n} \lambda_i b(v_i, w_i).$$

On vérifie que pour tous les éléments de la forme de (2.4), b' vaut zéro. Ainsi, deux fonctions de $F^{V\times W}$ dont la différence est un élément de R auront la même valeur par b'. On peut donc définir β par

$$\beta(z + R) := b'(z),$$

où $z + R \in F^{V\times W}/R$.

Comme on peut facilement vérifier la linéarité de b', on déduit la linéarité de β ainsi définie. Un calcul direct montre que $\beta \circ t = b$: pour $(v, w) \in V \times W$ on a

$$(\beta \circ t)(v, w) = \beta(v \otimes w) = \beta((v, w) + R) = b'(v, w) = b(v, w).$$

□

2.7 Corollaire. Soient U, V et W trois espaces vectoriels sur un corps F. Alors

(a) il existe un isomorphisme canonique de F-espaces vectoriels

$$V \otimes_F W \longrightarrow W \otimes_F V, \quad v \otimes w \longmapsto w \otimes v \ ;$$

(b) il existe un isomorphisme canonique de F-espaces vectoriels

$$F \otimes_F V \longrightarrow V, \quad \lambda \otimes v \longmapsto \lambda v \ ;$$

(c) le produit tensoriel est associatif, *i.e.* il existe un isomorphisme canonique de F-espaces vectoriels

$$\begin{array}{ccc} (U \otimes_F V) \otimes_F W & \longrightarrow & U \otimes_F (V \otimes_F W) \\ (u \otimes v) \otimes w & \longmapsto & u \otimes (v \otimes w)\ ; \end{array}$$

(d) il existe un isomorphisme canonique de F-espaces vectoriels

$$\begin{array}{ccc} U \otimes_F (V \oplus W) & \longrightarrow & (U \otimes_F V) \oplus (U \otimes_F W) \\ u \otimes (v, w) & \longmapsto & (u \otimes v, u \otimes w)\ ; \end{array}$$

(e) si V' et W' sont deux F-espaces vectoriels tels qu'il existe deux isomorphismes de F-espaces vectoriels

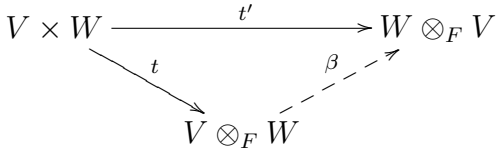
$$\pi_1 : V \xrightarrow{\cong} V', \quad \text{et} \quad \pi_2 : W \xrightarrow{\cong} W',$$

alors il existe un ismorphisme de F-espaces vectoriels

$$\begin{array}{ccc} V \otimes_F W & \longrightarrow & V' \otimes_F W' \\ v \otimes w & \longmapsto & \pi_1(v) \otimes \pi_2(w). \end{array}$$

PREUVE. *Partie* (a) : On note par t l'application de $V \times W \longrightarrow V \otimes_F W$ qui à (v, w) associe $v \otimes w$, et par t' l'application de $V \times W \longrightarrow W \otimes_F V$ qui à (v, w) associe $w \otimes v$.

Comme t' est une forme bilinéaire de $V \times W$ dans $W \otimes_F V$, on a, en appliquant la propriété universelle du produit tensoriel, l'existence d'une forme linéaire $\beta : V \otimes_F W \longrightarrow W \otimes_F V$ tel que le diagramme suivant



commute.

On a donc que pour $(v, w) \in V \times W$,

$$\beta(v \otimes w) = \beta(t(v, w)) = t'(v, w) = w \otimes v.$$

En renversant les rôles de V et de W, on obtient une autre forme linéaire $\gamma : W \times V \longrightarrow V \otimes_F W$ telle que $\gamma(w \otimes v) = v \otimes w$ pour $(v, w) \in V \times W$. On va voir que γ est l'inverse de β. Pour voir que $\gamma \circ \beta = \mathrm{Id}_{V \otimes_F W}$, il nous

suffit de vérifier que $(\gamma \circ \beta)(v \otimes w) = v \otimes w$ pour tout couple $(v, w) \in V \times W$, comme β et γ sont linéaires et que

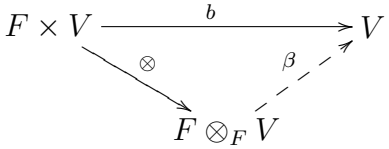
$$\{v \otimes w \mid (v, w) \in V \times W\}$$

engendre $V \otimes W$. Soit donc $(v, w) \in W \times V$, on calcule

$$(\gamma \circ \beta)(v \otimes w) = \gamma(w \otimes v) = v \otimes w.$$

De même, on vérifie que $\beta \circ \gamma = \mathrm{Id}_{W \otimes_F V}$; β est donc bien un isomorphisme.

Partie (b) : On définit $b : F \times V \longrightarrow V,\ (\lambda, v) \longmapsto \lambda v$; on vérifie que b est une forme bilinéaire, ainsi on a, par la propriété universelle du produit tensoriel, qu'il existe un unique homomorphisme de F-espaces vectoriels β tel que le diagramme suivant



commute. On a alors que pour $\lambda \otimes v \in F \otimes_F V$

$$\beta(\lambda \otimes v) = b(\lambda, v) = \lambda v,$$

comme voulu. Il nous reste à voir que β est bijectif. On définit $\gamma : V \longrightarrow F \otimes_F V$ qui associe à $v \in V$ le produit $1 \otimes v$. Voyons que γ ainsi définie est l'inverse de β, ce qui nous permettra de conclure.

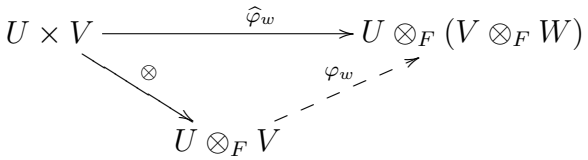
Il est clair que $\beta \circ \gamma = \mathrm{Id}_V$. Pour voir que $\gamma \circ \beta = \mathrm{Id}_{F \otimes_F V}$, il nous suffit de le voir sur tout couple $(f, v) \in F \times V$, comme γ et β sont linéaires et que les couples de cette forme engendrent $F \otimes_F V$. Soit donc $(f, v) \in F \times V$. On calcule

$$(\gamma \circ \beta)(f, v) = \gamma(fv) = 1 \otimes fv = f \otimes v.$$

Partie (c) : On commence par définir pour $w \in W$ arbitraire

$$\begin{array}{rccc} \widehat{\varphi}_w : & U \times V & \longrightarrow & U \otimes_F (V \otimes_F W) \\ & (u, v) & \longmapsto & u \otimes (v \otimes w). \end{array}$$

On vérifie que $\widehat{\varphi}_w$ est bilinéaire. On a donc, par la propriété universelle du produit tensoriel, qu'il existe une unique forme linéaire $\varphi_w : U \otimes_F V \longrightarrow U \otimes_F (V \otimes_F W)$ telle que le diagramme suivant



commute.

On définit maintenant une nouvelle fonction à partir de φ_w :

$$\begin{array}{rccc} \widehat{\varphi}: & (U \otimes_F V) \times W & \longrightarrow & U \otimes_F (V \otimes_F W) \\ & (x, w) & \longmapsto & \varphi_w(x). \end{array}$$

Il s'agit d'une forme bilinéaire. En effet, pour tout $x, y \in U \otimes_F V$, $w, w' \in W$, on a

$$\widehat{\varphi}(x+y, w) = \varphi_w(x+y) = \varphi_w(x) + \varphi_w(y) = \widehat{\varphi}(x, w) + \widehat{\varphi}(y, w),$$

comme φ_v est linéaire. Nous venons de voir que $\widehat{\varphi}$ est additive par rapport à sa première variable, nous pouvons donc nous contenter de vérifier les propriétés restantes pour $u \otimes v \in U \otimes_F V$. Soit $\lambda \in F$, on a

$$\begin{aligned} \widehat{\varphi}(\lambda u \otimes v, w) &= \varphi_w(\lambda u \otimes v) = \lambda \varphi_w(u \otimes v) = \lambda \widehat{\varphi}_w(u, v) \\ &= \lambda u \otimes (v \otimes w) = u \otimes (v \otimes (\lambda w)) = \widehat{\varphi}_{\lambda w}(u, v) \\ &= \varphi_{\lambda w}(u \otimes v) = \widehat{\varphi}(u \otimes v, \lambda w), \end{aligned}$$

et

$$\begin{aligned} \widehat{\varphi}(u \otimes v, w + w') &= \varphi_{w+w'}(u \otimes v) = \widehat{\varphi}_{w+w'}(u, v) = u \otimes (v \otimes (w + w')) \\ &= u \otimes (v \otimes w) + u \otimes (v \otimes w') = \widehat{\varphi}_w(u, v) + \widehat{\varphi}_{w'}(u, v) \\ &= \varphi_w(u \otimes v) + \varphi_{w'}(u \otimes v) = \widehat{\varphi}(u \otimes v, w) + \widehat{\varphi}(u \otimes v, w'). \end{aligned}$$

Donc par la propriété universelle du produit tensoriel, il existe une unique forme linéaire $\varphi : (U \otimes_F V) \otimes_F W \longrightarrow U \otimes_F (V \otimes_F W)$ telle que le diagramme suivant

$$\begin{array}{ccc} (U \otimes V) \times W & \xrightarrow{\quad\widehat{\varphi}\quad} & U \otimes_F (V \otimes_F W) \\ & {\scriptstyle\otimes}\searrow \quad \nearrow{\scriptstyle\varphi} & \\ & (U \otimes_F V) \otimes_F W & \end{array}$$

commute. Pour $(u, v, w) \in U \times V \times W$, on a

$$\varphi((u \otimes v) \otimes w) = \widehat{\varphi}(u \otimes v, w) = \varphi_w(u \otimes v) = \widehat{\varphi}_w(u, v) = u \otimes (v \otimes w).$$

Il nous reste à voir que φ est bijectif. Procédant de manière identique à ci-dessus, on obtient un forme linéaire $\gamma : U \otimes (V \otimes W) \longrightarrow (U \otimes V) \otimes W$ telle que

$$\gamma(u \otimes (v \otimes w)) = (u \otimes v) \otimes w.$$

Nous devons voir que γ est l'inverse de φ. Pour voir que $\gamma \circ \varphi = \mathrm{Id}_{(U \otimes_F V) \otimes_F W}$, il nous suffit de vérifier que $\gamma \circ \varphi$ est l'identité pour tout couple $(u \otimes v) \otimes w \in$

$(U \otimes_F V) \otimes_F W$, comme les éléments de cette forme engendrent $(U \otimes_F V) \otimes_F W$ et que γ et φ sont linéaires. On calcule

$$(\gamma \circ \varphi)((u \otimes v) \otimes w) = \gamma(u \otimes (v \otimes w)) = (u \otimes v) \otimes w,$$

ce qui montre que $\gamma \circ \varphi = \mathrm{Id}_{(U \otimes_F V) \otimes_F W}$; de même, on voit que $\varphi \circ \gamma = \mathrm{Id}_{U \otimes_F (V \otimes_F W)}$, ce qui permet de conclure que φ est bien l'isomorphisme de F-espace vectoriel que nous cherchions.

Partie (d) : on commence par définir $b : U \times (V \oplus W) \longrightarrow (U \otimes_F V) \oplus (U \otimes_F W)$ par

$$b(u, (v, w)) := (u \otimes v, u \otimes w).$$

Il est facile de vérifier que b ainsi défini est une forme bilinéaire. On a donc, par la propriété universelle du produit tensoriel qu'il existe une unique forme linéaire $\beta : U \otimes (V \oplus W) \longrightarrow (U \otimes_F V) \oplus (U \otimes_F W)$ telle que le diagramme suivant

$$\begin{array}{ccc} U \times (V \oplus W) & \xrightarrow{\quad b \quad} & (U \otimes_F V) \oplus (U \otimes_F W) \\ & {\scriptstyle \otimes} \searrow \quad \nearrow {\scriptstyle \beta} & \\ & U \otimes (V \oplus W) & \end{array}$$

commute. Ainsi, pour $u \in U$, $v \in V$ et $w \in W$, on a que

$$\beta(u \otimes (v, w)) = b(u, (v, w)) = (u \otimes v, u \otimes w).$$

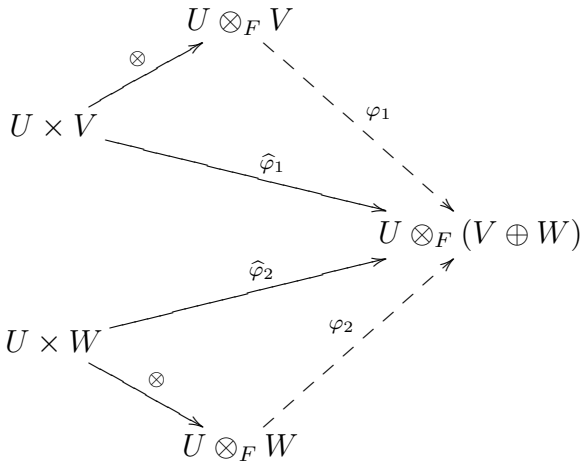
Il nous reste à voir que β est bijective. Pour définir un inverse à β, commençons par poser

$$\begin{array}{rccc} \widehat{\varphi}_1 : & U \times V & \longrightarrow & U \otimes_F (V \oplus W) \\ & (u, v) & \longmapsto & u \otimes (v, 0), \end{array}$$

et

$$\begin{array}{rccc} \widehat{\varphi}_2 : & U \times W & \longrightarrow & U \otimes_F (V \oplus W) \\ & (u, w) & \longmapsto & u \otimes (0, w). \end{array}$$

On vérifie facilement que ces deux fonctions sont bilinéaires. Par la propriété universelle du produit tensoriel, on obtient deux formes linéaires $\varphi_1 : U \otimes_F V \to U \otimes_F (V \oplus W)$ et $\varphi_2 : U \otimes_F W \to U \otimes_F (V \oplus W)$ telles que le diagramme suivant



commute. On définit alors

$$\begin{array}{rccc} \gamma : & (U \otimes_F V) \oplus (U \otimes_F W) & \longrightarrow & U \otimes_F (V \oplus W) \\ & (x, y) & \longmapsto & \varphi_1(x) + \varphi_2(y). \end{array}$$

Avec cette définition, on a que pour $u, u' \in U$, $v \in V$ et $w \in W$,

$$\begin{aligned} \gamma(u \otimes v, u' \otimes w) &= \varphi_1(u \otimes v) + \varphi_2(u' \otimes w) = \widehat{\varphi}_1(u, v) + \widehat{\varphi}_2(u', w) \\ &= u \otimes (v, 0) + u' \otimes (0, w). \end{aligned}$$

Voyons que γ est l'inverse de β. Pour voir que $\gamma \circ \beta = \mathrm{Id}_{U \otimes_F (V \oplus W)}$, il nous suffit de faire la vérification sur les éléments de la forme $u \otimes (v, w) \in U \otimes_F (V \oplus W)$, comme ils engendrent $U \otimes_F (V \oplus W)$ et que β et γ sont linéaires. On calcule

$$\begin{aligned} (\gamma \circ \beta)(u \otimes (v, w)) &= \gamma(u \otimes v, u \otimes w) = u \otimes (v, 0) + u \otimes (0, w) \\ &= u \otimes ((v, 0) + (0, w)) = u \otimes (v, w). \end{aligned}$$

i.e. $\gamma \circ \beta = \mathrm{Id}_{U \otimes_F (V \oplus W)}$. Pour voir l'autre condition, nous pouvons à nouveau nous contenter de faire la vérification sur les éléments de la forme $(u \otimes v, u' \otimes w) \in (U \otimes_F V) \oplus (U \otimes_F W)$. On calcule

$$\begin{aligned} (\beta \circ \gamma)(u \otimes v, u' \otimes w) &= \beta(u \otimes (v, 0) + u' \otimes (0, w)) \\ &= (u \otimes v, 0) + (0, u' \otimes w) = (u \otimes v, u' \otimes w), \end{aligned}$$

ce qui finit de montrer le bijectivité de β.

Partie (e) : on définit une forme bilinéaire $b : V \times W \longrightarrow V' \otimes_F W'$ par $b(v, w) = \pi_1(v) \otimes \pi_2(w)$. Par la propriété universelle de produit tensoriel, on obtient une forme linéaire $\beta : V \otimes_F W \longrightarrow V' \otimes_F W'$ telle que pour $(v, w) \in V \times W$

$$\beta(v \otimes w) = b(v, w) = \pi_1(v) \otimes \pi_2(w).$$

En inversant les rôles de V, W et de V', W', on obtient une forme linéaire $\gamma : V' \otimes_F W' \longrightarrow V \otimes_F W$ telle que pour $v' \otimes w' \in V' \otimes_F W'$

$$\gamma(v' \otimes w') = \pi_1^{-1}(v') \otimes \pi_2^{-1}(w').$$

On vérifie facilement que γ est l'inverse de β pour pouvoir conclure. □

Soient V et W deux espaces vectoriels sur un corps F de bases respectives $(v_1, \ldots, v_n)$ et $(w_1, \ldots, w_m)$. On a alors, en utilisant les parties (d) et (e) du corollaire, que

$$V \otimes_F W \cong \left(\bigoplus_{i=1}^{n} Fv_i \right) \otimes_F \left(\bigoplus_{i=1}^{m} Fw_i \right) \cong \bigoplus_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} Fv_i \otimes_F Fw_j.$$

Ainsi, $\dim(V \otimes_F W) = \dim(V)\dim(W)$, comme la dimension de $Fv_i \otimes Fw_j$ est 1 pour tout $i = 1, \ldots, n$ et $j = 1, \ldots, m$; en effet en utilisant les parties (b) et (e) du corollaire, on a

$$Fv_i \otimes_F Fw_j \cong F \otimes_F F \cong F$$

La liste $(v_i \otimes w_j)_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}}$ contient $\dim(V \otimes_F W)$ vecteurs et engendre $V \otimes_F W$, il s'agit donc d'une base de $V \otimes_F W$.

Algèbre sur le Produit Tensoriel

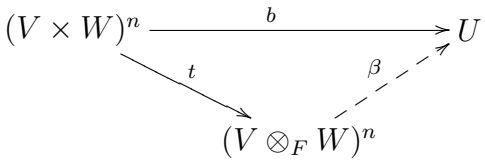
Soient A et B deux algèbres sur un corps F ; on considère leur produit tensoriel $A \otimes_F B$, qui est un F-espace vectoriel que l'on peut doter d'une multiplication qui en fasse une F-algèbre, comme nous allons le voir grâce à la proposition suivante.

2.8 Proposition. Soient n un entier positif, V, W et U trois F-espaces vectoriels et $b : (V \times W)^n \to U$ une forme multilinéaire en $2n$ variables.

Soit encore $t : (V \times W)^n \to (V \otimes_F W)^n$ la forme définie par

$$t(v_1, w_1, \ldots, v_n, w_n) := (v_1 \otimes w_1, \ldots, v_n \otimes w_n).$$

Alors, il existe une unique forme multilinéaire à n variables $\beta : (V \otimes_F W)^n \to U$ telle que le diagramme suivant



commute.

PREUVE. Nous utilisons les mêmes idées que dans la preuve de la propriété universelle du produit tensoriel.

Premièrement, on remarque que l'unicité est claire, car si

$$z = \left(\sum_{i_1=1}^{k_1} v_{i_1}^{(1)} \otimes w_{i_1}^{(1)}, \cdots, \sum_{i_n=1}^{k_n} v_{i_n}^{(n)} \otimes w_{i_n}^{(n)} \right) \in (V \otimes_F W)^n,$$

alors on doit avoir

$$\begin{aligned} \beta(z) &= \sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} \beta(v_{i_1}^{(1)} \otimes w_{i_1}^{(1)}, \ldots, v_{i_n}^{(n)} \otimes w_{i_n}^{(n)}) \\ &= \sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} b(v_{i_1}^{(1)}, w_{i_1}^{(1)}, \ldots, v_{i_n}^{(n)}, w_{i_n}^{(n)}), \end{aligned}$$

qui est déterminé de manière unique.

On définit maintenant $b' : (F^{V \times W})^n \to U$ par

$$\begin{aligned} &\left(\sum_{i_1=1}^{k_1} \lambda_{i_1}^{(1)}(v_{i_1}^{(1)}, w_{i_1}^{(1)}), \ldots, \sum_{i_n=1}^{k_n} \lambda_{i_n}^{(n)}(v_{i_n}^{(n)}, w_{i_n}^{(n)}) \right) \\ &\qquad \overset{b'}{\longmapsto} \sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} \lambda_{i_1}^{(1)} \cdots \lambda_{i_n}^{(n)} b(v_{i_1}^{(1)}, w_{i_1}^{(1)}, \ldots, v_{i_n}^{(n)}, w_{i_n}^{(n)}). \end{aligned}$$

On vérifie que b' est multilinéaire (en n variables) et que si dans

$$x = (x_1, \ldots, x_n) \in (F^{V \times W})^n$$

un des x_i est une des formes de (2.4), alors $b'(x) = 0$. Ainsi, si x et y dans $(F^{V \times W})^n$ ont leurs composantes prises deux-à-deux toujours séparées par un élément de R (avec R défini de la même manière que dans (2.3)), alors $b'(x) = b'(y)$. On peut donc définir $\beta : (V \otimes W)^n \to U$ par

$$z = (z_1 + R, \ldots, z_n + R) \overset{\beta}{\longmapsto} b'(z_1, \ldots, z_n),$$

pour $z \in (V \otimes W)^n$. La multilinéarité de β découle de celle de b' et un calcul direct montre que $\beta \circ t = b$. □

Avec la proposition, on peut définir une opération de multiplication dans le produit tensoriel de deux algèbres A et B (sur un corps F).

Pour ce faire, on commence par définir un forme multilinéaire

$$b : (A \times B)^2 \to A \otimes_F B$$

par

$$b(a, b, c, d) := (ac) \otimes (bd).$$

On applique alors la proposition pour obtenir une forme bilinéaire

$$\beta : (A \otimes_F B)^2 \to A \otimes_F B$$

telle que, pour $\sum_{i=1}^{n} a_i \otimes b_i$ et $\sum_{j=1}^{m} c_j \otimes d_j$ dans $A \otimes_F B$,

$$\beta\left(\sum_{i=1}^{n} a_i \otimes b_i, \sum_{j=1}^{m} c_j \otimes d_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} b(a_i, b_i, c_j, d_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} (a_i c_i) \otimes (b_j d_j).$$

2.9 Définition. On appelle l'opération

$$\beta : (A \otimes_F B)^2 \to A \otimes_F B,$$

construite ci-dessus, la **multiplication** et on la note par juxtaposition.

Vérifions que cette opération de multiplication donne bien un structure d'algèbre à $A \otimes_F B$.

Premièrement, il est clair que l'identité pour la multiplication est $1 \otimes 1$.

De plus, β bilinéaire implique la distributivité à gauche et à droite de la multiplication par rapport à l'addition.

Similairement, β bilinéaire implique que pour $x, y \in A \otimes_F B$ et $\lambda \in F$,

$$\lambda(xy) = (\lambda x)y = x(\lambda y).$$

Comme nous savons que la multiplication est distributive par rapport à l'addition, il nous suffit de vérifier son associativité pour le triplet

$$a \otimes b,\ c \otimes d,\ e \otimes f \in A \otimes_F B.$$

On calcule

$$\begin{aligned}((a \otimes b)(c \otimes d))(e \otimes f) &= (ac \otimes bd)(e \otimes f) = ace \otimes bdf \\ &= (a \otimes b)(ce \otimes df) = (a \otimes b)((c \otimes d)(e \otimes f)).\end{aligned}$$

Centre du Produit Tensoriel d'Algèbres

2.10 Proposition. Soient U et V deux F-espaces vectoriels et deux listes de vecteurs $u_1, \ldots, u_n \in U$ et $v_1, \ldots, v_n \in V$.

Si les u_i sont linéairement indépendants et si $\sum_{i=1}^{n} u_i \otimes v_i = 0$. Alors

$$v_i = 0 \quad \text{pour tout } i = 1, \ldots, n.$$

PREUVE. (*tirée de [2, p. 367-368]*) À toute forme bilinéaire $f : U \times V \to F$, on peut associer (par la propriété universelle du produit tensoriel) une forme linéaire $\tau : U \otimes_F W \to F$ telle que $\tau \circ \otimes = f$. On a donc

$$0 = \tau\left(\sum_{i=1}^{n} u_i \otimes v_i\right) = \sum_{i=1}^{n} f(u_i, v_i),$$

pour une forme bilinéaire $f : U \times V \to F$ quelconque. En particulier, si $\alpha \in U^*$ et $\beta \in V^*$, alors on peut définir f par

$$f(u, v) = \alpha(u)\beta(v) \quad \text{pour } (u, v) \in U \times V,$$

et on a ainsi

$$\sum_{i=1}^{n} \alpha(u_i)\beta(v_i) = 0.$$

Comme les u_i sont linéairement indépendants, on peut toujours trouver, pour $j = 1, \ldots, n$, un $\alpha \in U^*$ tel que

$$\alpha(u_i) = \delta_{ij}.$$

Ainsi, on a

$$\beta(v_j) = 0 \quad \text{pour tout } j = 1, \ldots, n.$$

Ceci étant vrai pour tout $\beta \in V^*$, on peut conclure. □

La proposition (2.10) permet de retrouver le résultat que nous avons vu à la fin de la section sur la propriété universelle du produit tensoriel, tout en l'étendant au cas d'espaces vectoriels de dimension infinie.

En effet, si V et W sont deux F-espaces vectoriels de F-bases respectives $\{v_i \mid i \in I\}$ et $\{w_j \mid j \in J\}$ (avec I et J deux ensembles d'indices quelconques). Pour tout $x = \sum_k a_k \otimes b_k \in V \otimes_F W$, on peut toujours trouver des $a_{k,n} \in F$ et des $b_{k,m} \in F$ en nombre fini tels que

$$x = \sum_{k,n,m} a_{k,n} b_{k,m} (v_n \otimes w_m) = \sum_{n,m} \left(\sum_k a_{k,n} b_{k,m}\right) (v_n \otimes w_m),$$

et la proposition (2.10) nous dit alors qu'il n'existe qu'un choix possible de coefficents $\sum_k a_{k,n}b_{k,m}$. En effet, si

$$\sum_{n,m} c_{n,m}(v_n \otimes w_m) = \sum_{n,m} d_{n,m}(v_n \otimes w_m),$$

avec $c_{n,m}$ et $d_{n,m}$ dans F, alors on a que

$$0 = \sum_{n,m}(c_{n,m} - d_{n,m})(v_n \otimes w_m) = \sum_m \left(\left(\sum_n (c_{n,m} - d_{n,m})v_n \right) \otimes w_m \right)$$

et comme les w_m sont F-linéairement indépendants, on a pour tout m,

$$0 = \sum_n (c_{n,m} - d_{n,m})v_n,$$

comme les v_n sont F-linéairement indépendants, on a

$$c_{n,m} = d_{n,m}$$

pour tout n, m. Ainsi, les $v_n \otimes w_m$ forment une base du F-espace vectoriel de $V \otimes_F W$.

2.11 Proposition. Soit A et B deux algèbres sur un corps F. Alors on a l'égalité

$$\mathcal{Z}(A \otimes_F B) = \mathcal{Z}(A) \otimes_F \mathcal{Z}(B),$$

en identifiant $\mathcal{Z}(A) \otimes_F \mathcal{Z}(B)$ à

$$Z := \left\{ \sum_i a_i \otimes b_i \;\middle|\; a_i \in \mathcal{Z}(A) \text{ et } b_i \in \mathcal{Z}(B) \right\} \subseteq A \otimes_F B.$$

par un isomorphisme de F-algèbres.

(Comme $\mathcal{Z}(A) \otimes_F \mathcal{Z}(B)$ et Z ont pour base les produits tensoriels (dans $\mathcal{Z}(A) \otimes_F \mathcal{Z}(B)$ et $A \otimes_F B$ respectivement) d'éléments d'une base de $\mathcal{Z}(A)$ et d'une base de $\mathcal{Z}(B)$, cette identification est immédiate.)

Preuve. L'inclusion $Z \subseteq \mathcal{Z}(A \otimes_F B)$ est claire. En effet, si $z = \sum_i a_i \otimes b_i$ avec $a_i \in \mathcal{Z}(A)$ et $b_i \in \mathcal{Z}(B)$ et si $y = \sum_j c_j \otimes d_j \in A \otimes_F B$, alors on a

$$z \cdot y = \sum_{i,j} (a_i c_j) \otimes (b_i d_j) = \sum_{i,j} (c_j a_i) \otimes (d_j b_i) = z \cdot y.$$

Pour voir l'inclusion $Z \supseteq \mathcal{Z}(A \otimes_F B)$, choisissons $x = \sum_i a_i \otimes b_i \in \mathcal{Z}(A \otimes_F B)$ et $\{e_j \mid j \in J\}$ une base de B en tant que F-espace vectoriel,

avec J un ensemble d'indices. Pour tout b_i, il existe un liste nulle presque partout de $\lambda_{ij} \in F$ avec j parcourant J tels que

$$b_i = \sum_j \lambda_{ij} e_j.$$

On a donc

$$x = \sum_i \left(a_i \otimes \left(\sum_j \lambda_{ij} e_j \right) \right) = \sum_j \left(\sum_i (\lambda_{ij} a_i) \otimes e_j \right).$$

On définit $\tilde{a}_j := \sum_i (\lambda_{ij} a_i)$, qui est uniquement déterminé par x et les e_j. En effet, s'il existe des $\bar{a}_j \in A$ tels que

$$\sum_j \tilde{a}_j \otimes e_j = \sum_j \bar{a}_j \otimes e_j,$$

alors on a

$$\sum_j (\tilde{a}_j - \bar{a}_j) \otimes e_j = 0,$$

et la proposition (2.10) nous donne $\tilde{a}_j = \bar{a}_j$ pour tout j.

Soit $a \in A$, on a $(a \otimes 1) \cdot x = x \cdot (a \otimes 1)$, *i.e.*

$$(a \otimes 1) \cdot \left(\sum_j \tilde{a}_j \otimes e_j \right) = \left(\sum_j \tilde{a}_j \otimes e_j \right) \cdot (a \otimes 1),$$

et donc

$$\sum_j (a\tilde{a}_j) \otimes e_j = \sum_j (\tilde{a}_j a) \otimes e_j,$$

avec la proposition(2.10) on peut conclure que $a\tilde{a}_j = \tilde{a}_j a$. Ceci étant vrai pour tout $a \in A$, on a $\tilde{a}_j \in \mathcal{Z}(A)$ pour tout j.

Soit $\{c_k \mid k \in K\}$ une base de $\mathcal{Z}(A)$ comme F-espace vectoriel, avec K un ensemble d'indices. Pour tout $\tilde{a}_j$, on peut trouver un liste nulle presque partout de $\mu_{jk} \in F$ avec k parcourant K tels que

$$\tilde{a}_j = \sum_k \mu_{jk} c_k,$$

ainsi

$$x = \sum_j \tilde{a}_j \otimes e_j = \sum_j \left(\sum_k \mu_{jk} c_k \right) \otimes e_j = \sum_k c_k \otimes \left(\sum_j \mu_{jk} e_j \right)$$

Définissons $\tilde{b}_k := \sum_j \mu_{jk} e_j$. Par un raisonnement similaire à celui développé pour les $\tilde{a}_j$, on a que les $\tilde{b}_i$ sont uniquement déterminés par x et les c_i ; et on déduit aussi de la même manière que ci-dessus que les $\tilde{b}_i$ sont dans $\mathcal{Z}(B)$. Comme les c_k sont dans $\mathcal{Z}(A)$, on a donc montré que

$$\mathcal{Z}(A \otimes_F B) \subseteq Z,$$

comme voulu. □

2.12 Corollaire. Soit F un corps et A, B deux algèbres F-centrales. Alors $A \otimes_F B$ est aussi F-centrale.

PREUVE. On a

$$\begin{array}{ccccc} \mathcal{Z}(A \otimes_F B) & \cong & \mathcal{Z}(A) \otimes_F \mathcal{Z}(B) & = & (F1) \otimes_F (F1) \\ & \cong & F \otimes_F F & \cong & F. \\ & \uparrow & & \uparrow & \\ & \text{(e) de (2.7)} & & \text{(b) de (2.7)} & \end{array}$$

□

Produit Tensoriel d'Algèbres Simples

2.13 Proposition. Soit A et B deux algèbres simples sur un corps F, telles que A soit F-centrale. Alors $A \otimes_F B$ est aussi simple.

PREUVE. Soit I un idéal bilatère non-zéro de $A \otimes_F B$. Notre but est de montrer que $I = A \otimes_F B$.

Soit $x \in I$ s'écrivant comme $x = \sum_{i=1}^{n} a_i \otimes b_i$, pour un certain $n \geq 1$. Dans l'écriture de x, on peut toujours substituer aux b_i leur décomposition dans une F-base de B. Ainsi, on obtient un nouvelle expression de x où tous les éléments de B entrant en jeu sont, en particulier, F-linéairement indépendants entre eux. On peut donc définir un entier m comme suit :

Soit $m \geq 1$ l'entier minimal tel qu'il existe un $x \in I$ non-zéro satisfaisant

$$x = \sum_{i=1}^{m} a_i \otimes b_i,$$

avec $a_1, \ldots, a_m$ dans A quelconques et $b_1, \ldots, b_m$ dans B F-linéairement indépendants.

La minimalité de m implique que tous les a_i sont non-zéro. Comme Aa_1A est un idéal bilatère non-zéro de A, on a $Aa_1A = A$. Il existe donc

$(g_j, h_j)_{j=1,\dots,n} \subseteq A \times A$ tels que $\sum_{j=1}^n g_j a_1 h_j = 1$. On a

$$I \ni \sum_{j=1}^n \underbrace{(g_j \otimes 1) \cdot x \cdot (h_j \otimes 1)}_{\in I} = \sum_{j=1}^n \sum_{i=1}^m (g_j a_i h_j) \otimes b_i = \sum_{i=1}^m \left(\sum_{j=1}^n g_j a_i h_j \right) \otimes b_i,$$

ainsi on peut supposer que $a_1 = 1$.

Par l'absurde, supposons maintenant que $m > 1$. Dans ce cas, on doit avoir $a_2 \in A \setminus F$. En effet, si $a_2 \in F$, alors au risque de remplacer b_2 par $a_2^{-1} b_2$, on a $a_2 = 1$, et donc

$$x = 1 \otimes (b_1 + b_2) + \sum_{i=3}^m a_i \otimes b_i,$$

et comme $(b_1 + b_2), b_3, b_4, \dots, b_m$ est F-linéairement indépendante, cette équation contredit la minimalité de m. Ainsi on a $a_2 \in A \setminus F$.

Comme A est F-centrale, il existe un $z \in A$ tel que $z a_2 \neq a_2 z$, on a alors

$$\begin{aligned} I \ni (z \otimes 1) \cdot x - x \cdot (z \otimes 1) &= \sum_{i=1}^m (z a_i) \otimes b_i - \sum_{i=1}^m (a_i z) \otimes b_i \\ &= \sum_{i=1}^m (z a_i - a_i z) \otimes b_i \\ &= 0 \otimes b_1 + \underbrace{(z a_2 - a_2 z)}_{\neq 0} \otimes b_2 + \sum_{i=3}^m (z a_i - a_i z) \otimes b_i, \end{aligned}$$

ce qui contredit la minimalité de m. Ainsi on doit avoir $m = 1$.

On sait maintenant que x s'écrit comme $1 \otimes b$ pour un certain $b \in B$ non-nul. Comme B est simple, on a $BbB = 1$. On peut donc trouver $(r_j, s_j)_{i=1,\dots,n} \subseteq B \times B$ tels que $\sum_{j=1}^n r_j b s_j = 1$, et par conséquent

$$I \ni \sum_{j=1}^n \underbrace{(1 \otimes r_j) \cdot (1 \otimes b) \cdot (1 \otimes s_j)}_{\in I} = \sum_{j=1}^n 1 \otimes (r_j b s_j) = 1 \otimes \left(\sum_{j=1}^n r_j b s_j \right) = 1 \otimes 1,$$

d'où on conclut que $I = A \otimes_F B$, comme voulu. □

2.14 Définition. Soit A une algèbre sur un corps F. On dit que A est **centrale simple** sur F si A est simple et F-centrale.

2.15 Théorème sur les algèbres centrales simples. Soient A et B deux algèbres sur un corps F. On a l'implication

$$A, B \text{ centrales simples sur } F \quad \Longrightarrow \quad A \otimes_F B \text{ centrale simple sur } F.$$

PREUVE. On applique (2.12) et (2.13) ensemble. □

Chapitre 3

Groupe de Brauer

3.1 Propriétés. Soit A une algèbre *simple* de dimension finie sur un corps F et $m, n \in \mathbb{N}$. Alors

(a) il existe un isomorphisme de F-algèbres

$$\begin{array}{rccc} \Phi : & A \otimes_F \mathbb{M}_n(F) & \longrightarrow & \mathbb{M}_n(A) \\ & a \otimes (c_{ij})_{i,j=1,\dots,n} & \longmapsto & (c_{ij})_{i,j=1,\dots,n} \cdot a := (c_{ij}a)_{i,j=1,\dots,n} \ ; \end{array}$$

(b) $\mathbb{M}_n(A)$ est simple ;

(c) si A est centrale simple sur F, alors $\mathbb{M}_n(A)$ est aussi centrale simple sur F ;

(d) il existe un isomorphisme de F-algèbres

$$\begin{array}{rccc} \Psi : & \mathbb{M}_n(A) \otimes_F \mathbb{M}_m(F) & \longrightarrow & \mathbb{M}_{nm}(A) \\ & M \otimes (c_{ij})_{i,j=1,\dots,m} & \longmapsto & \begin{pmatrix} c_{1,1}M & \cdots & c_{1,m}M \\ \vdots & & \vdots \\ c_{m,1}M & \cdots & c_{m,m}M \end{pmatrix} . \end{array}$$

Preuve. *Partie* (a) : On définit $f : A \times \mathbb{M}_n(F) \longrightarrow \mathbb{M}_n(A)$ par

$$(a, (c_{ij})_{i,j=1,\dots,n}) \overset{f}{\longmapsto} (c_{ij}a)_{i,j=1,\dots,n}$$

qui est une forme bilinéaire. On a, par la propriété universelle du produit tensoriel, une forme linéaire $\Phi : A \otimes_F \mathbb{M}_n(F) \longrightarrow \mathbb{M}_n(A)$ tel que $f = \Phi \circ \otimes$. Ainsi

$$a \otimes (c_{ij})_{i,j=1,\dots,n} \overset{\Phi}{\longmapsto} (c_{ij}a)_{i,j=1,\dots,n}.$$

est bien définie, et il nous faut maintenant voir qu'il s'agit d'un isomorphisme de F-algèbres.

Pour avoir que Φ est un homomorphisme de F-algèbres, on remarque que pour $a, \tilde{a} \in A$ et $m, \tilde{m} \in \mathbb{M}_n(F)$

$$\begin{aligned}\Phi((a \otimes m) \cdot (\tilde{a} \otimes \tilde{m})) &= \Phi((a\tilde{a}) \otimes (m\tilde{m})) = (m\tilde{m})(a\tilde{a}) \\ &= (ma)(\tilde{m}\tilde{a}) = \Phi(a \otimes m)\Phi(\tilde{a} \otimes \tilde{m}),\end{aligned}$$

comme les coefficents des matrices m et $\tilde{m}$ commutent avec les éléments de A.

Pour voir que Φ est bijective, on remarque que

$$\begin{aligned}\dim_F(A \otimes_F \mathbb{M}_n(F)) &= \dim_F(A) \cdot \dim_F(\mathbb{M}_n(F)) = \dim_F(A) \cdot n^2 \\ &= \dim_F(\mathbb{M}_n(A)),\end{aligned}$$

ainsi, il suffit de voir la surjectivité de Φ. Soit $m \in \mathbb{M}_n(A)$. Il existe des coefficients $m_{ij} \in A$ tels que (avec les notations de (1.17)) $m = \sum_{i,j=1}^n E_{ij} m_{ij}$. Ainsi

$$\Phi\left(\sum_{i,j=1}^n m_{ij} \otimes E_{ij}\right) = \sum_{i,j=1}^n E_{ij} m_{ij} = m.$$

Partie (b) : On applique (1.19) et la partie (b) de (1.21) pour avoir $\mathbb{M}_n(F)$ centrale simple sur F. On peut alors utiliser (2.13).

Partie (c) : On a vu en (b) que $\mathbb{M}_n(F)$ est centrale simple sur F. On peut donc appliquer (2.15).

Partie (d) : Si on arrive à montrer que $\mathbb{M}_n(A)$ est une F-algèbre simple, alors on pourra appliquer la partie (a) pour avoir l'isomorphisme de F-algèbres

$$\begin{array}{rccc}\Phi : & \mathbb{M}_n(A) \otimes_F \mathbb{M}_m(F) & \longrightarrow & \mathbb{M}_m(\mathbb{M}_n(A)) \\ & M \otimes (c_{ij})_{i,j=1,\ldots,m} & \longmapsto & (c_{ij})_{i,j=1,\ldots,m} \cdot M := (c_{ij}M)_{i,j=1,\ldots,m}.\end{array}$$

et comme on peut identifier $\mathbb{M}_m(\mathbb{M}_n(A))$ et $\mathbb{M}_{nm}(A)$, cela permettra de conclure.

Il faut donc voir que $\mathbb{M}_n(A)$ est simple. On sait, par le théorème de Wedderburn (1.40), qu'il existe un F-corps gauche D tel que $A \cong \mathbb{M}_l(D)$ pour un certain entier l. Ainsi, $\mathbb{M}_n(A) \cong \mathbb{M}_n(\mathbb{M}_l(D)) \cong \mathbb{M}_{nl}(D)$, qui est simple par (1.19). □

3.2 Proposition. Soit A une algèbre sur un corps F. Alors

(a) il existe un homomorphisme de F-algèbres

$$\Phi : A \otimes_F A^{\mathrm{op}} \longrightarrow \mathrm{End}_F(A), \quad a \otimes b \longmapsto \begin{cases} A \to A \\ x \mapsto axb \, ; \end{cases}$$

(b) Si A est centrale simple sur F avec $\dim_F(A) = n < \infty$, alors Φ est un isomorphisme de F-algèbres et on a les isomorphismes de F-algèbres

$$A \otimes_F A^{\mathrm{op}} \cong \mathrm{End}_F(A) \cong \mathbb{M}_n(F).$$

PREUVE. *Partie* (a) : Comme d'habitude, on commence par définir une forme bilinéaire

$$f : A \times A^{\mathrm{op}} \longrightarrow \mathrm{End}_F(A), \quad (a, b) \longmapsto \begin{cases} A \to A \\ x \mapsto axb, \end{cases}$$

et la propriété universelle du produit tensoriel nous donne alors que Φ est une forme linéaire bien définie.

On choisit alors $a, \tilde{a} \in A$ et $b, \tilde{b} \in A^{\mathrm{op}}$, et on calcule

$$\begin{aligned} \Phi((a \otimes b) \cdot (\tilde{a} \otimes \tilde{b})) &= \Phi((a \cdot \tilde{a}) \otimes (b \cdot_{\mathrm{op}} \tilde{b})) = \Phi((a \cdot \tilde{a}) \otimes (\tilde{b} \cdot b)) \\ &= (x \mapsto a\tilde{a}x\tilde{b}b) = (x \mapsto axb) \circ (x \mapsto \tilde{a}x\tilde{b}) \\ &= \Phi(a \otimes b) \circ \Phi(\tilde{a} \otimes \tilde{b}). \end{aligned}$$

Partie (b) : Commençons par voir que Φ est bijective. On remarque que

$$\dim_F(A \otimes_F A^{\mathrm{op}}) = \dim_F(A)^2 = \dim_F(\mathrm{End}_F(A)),$$

il nous suffit donc de voir l'injectivité. Comme A est centrale simple sur F, le théorème (2.15), nous donne que $A \otimes_F A^{\mathrm{op}}$ est centrale simple sur F. Or $\mathrm{Ker}(\Phi)$ est un idéal bilatère de $A \otimes_F A^{\mathrm{op}}$, et, comme $\Phi \neq 0$, on a l'injectivité. Ainsi, Φ est un isomorphisme de F-algèbres.

La proposition (1.29), nous donne l'isomorphisme de F-algèbres

$$\mathrm{End}_F(A) \cong \mathbb{M}_n(F),$$

et nous permet de conclure. □

Soit un corps F et A, B deux F-algèbres centrales simples sur F avec $\dim_F(A), \dim_F(B) < \infty$. On définit la relation d'équivalence

$$A \sim B \quad \Longleftrightarrow \quad A \otimes_F \mathbb{M}_r(F) \cong B \otimes_F \mathbb{M}_s(F),$$

en tant que F-algèbres, pour un certain couple $(r, s) \in \mathbb{N} \times \mathbb{N}$.

La réflexivité et la symétrie sont évidentes. Pour voir la transitivité, il suffit d'utiliser la partie (d) de (3.1) (dans le cas particulier où $A = F$). En effet, si A, B, C sont trois F-algèbres centrales simples sur F avec

$$A \otimes_F \mathbb{M}_r(F) \cong B \otimes_F M_s(F) \quad \text{et} \quad B \otimes_F M_t(F) \cong C \otimes_F \mathbb{M}_u(F),$$

pour certains $r, s, t, u \in \mathbb{N}$, alors

$$\begin{aligned} A \otimes_F \mathbb{M}_{rt}(F) &\cong A \otimes_F \mathbb{M}_r(F) \otimes_F \mathbb{M}_t(F) \cong B \otimes_F \mathbb{M}_s(F) \otimes_F \mathbb{M}_t(F) \\ &\cong B \otimes_F \mathbb{M}_t(F) \otimes_F \mathbb{M}_s(F) \cong C \otimes_F \mathbb{M}_u(F) \otimes_F \mathbb{M}_s(F) \\ &\cong C \otimes_F \mathbb{M}_{us}(F). \end{aligned}$$

On note par $[A]$ la classe d'équivalence de A.

3.3 Définition. On appelle **groupe de Brauer** l'ensemble $\mathrm{Br}(F)$ de toutes les classes d'équivalence des F-algèbres de dimension finie centrales simples sur F.

On définit une opération de multiplication $\cdot$ sur $\mathrm{Br}(F)$ par

$$[A] \cdot [B] := [A \otimes_F B].$$

3.4 Théorème. La multiplication $\cdot$ est bien définie et donne une structure de groupe abélien à $\mathrm{Br}(F)$.

Preuve. *Bien défini* : Si $A, \tilde{A}, B, \tilde{B}$ sont quatre F-algèbres centrales simples sur F telles que pour certains $r, \tilde{r}, s, \tilde{s} \in \mathbb{N}$

$$A \otimes_F \mathbb{M}_r(F) \cong \tilde{A} \otimes_F \mathbb{M}_{\tilde{r}}(F) \quad \text{et} \quad B \otimes_F \mathbb{M}_s(F) \cong \tilde{B} \otimes_F \mathbb{M}_{\tilde{s}}(F),$$

alors

$$\begin{aligned} A \otimes_F B \otimes_F \mathbb{M}_{rs}(F) &\cong (A \otimes_F \mathbb{M}_r(F)) \otimes_F (B \otimes_F \mathbb{M}_s(F)) \\ &\cong (\tilde{A} \otimes_F \mathbb{M}_{\tilde{r}}(F)) \otimes_F (\tilde{B} \otimes_F \mathbb{M}_{\tilde{s}}(F)) \\ &\cong \tilde{A} \otimes_F \tilde{B} \otimes_F \mathbb{M}_{\tilde{r}\tilde{s}}(F). \end{aligned}$$

Associativité : si A, B, C sont trois F-algèbres centrales simples sur F, alors

$$([A] \cdot [B]) \cdot [C] = [(A \otimes_F B) \otimes_F C] = [A \otimes_F (B \otimes_F C)] = [A] \cdot ([B] \cdot [C]).$$

Élément neutre : Si A est une F-algèbre centrale simple sur F, alors avec (b) de (2.7)

$$[A] \cdot [F] = [A \otimes_F F] = [A].$$

Inverse : Si A est une F-algèbre centrale simple sur F, alors avec (b) de (3.2)

$$[A] \cdot [A^{\mathrm{op}}] = [A \otimes_F A^{\mathrm{op}}] = [\mathbb{M}_n(F)] = [F] = 1_{\mathrm{Br}(F)}.$$

Commutativité : si A, B sont deux F-algèbres centrales simples sur F, alors

$$[A] \cdot [B] = [A \otimes_F B] = [B \otimes_F A] = [B] \cdot [A].$$

□

3.5 Proposition. Soit un corps F et A, B deux F-algèbres centrales simples sur F de dimension finie.

Le théorème de Wedderburn (1.40) nous donne $n, m \in \mathbb{N}$ et D, E deux F-corps gauches tels que

$$A \cong \mathbb{M}_n(D) \quad \text{et} \quad B \cong \mathbb{M}_m(E),$$

en tant que F-algèbres. Alors

(a) D et E sont centrales simples sur F ;

(b) $A \sim B \iff D \cong E$;

(c) Si $N, M \in [A]$ sont deux corps gauches, alors $N \cong M$ en tant que F-algèbres.

Preuve. *Partie* (a) : Tout corps gauche est simple.

Comme A est F-centrale, $\mathcal{Z}(\mathbb{M}_n(D)) = F\mathbb{1}_n$. Or $x \in \mathcal{Z}(D)$ implique $x \cdot \mathbb{1}_n \in \mathcal{Z}(\mathbb{M}_n(D))$; par cette inclusion, on a

$$\dim_F(\mathcal{Z}(D)) \leq \dim_F(\mathcal{Z}(\mathbb{M}_n(D))) = 1,$$

et donc D est F-central.

Partie (b) : $\boxed{\Rightarrow}$ On a deux entiers $r, s \in \mathbb{N}$ tels que $A \otimes_F \mathbb{M}_r(F) \cong B \otimes_F \mathbb{M}_s(F)$. Ainsi $\mathbb{M}_n(D) \otimes_F \mathbb{M}_r(F) \cong \mathbb{M}_m(E) \otimes_F \mathbb{M}_s(F)$, or

$$\mathbb{M}_n(D) \otimes_F \mathbb{M}_r(F) \cong D \otimes_F \mathbb{M}_n(F) \otimes_F \mathbb{M}_r(F) \cong D \otimes_F \mathbb{M}_{nr}(F) \cong \mathbb{M}_{nr}(D),$$

et, en raisonnant de même sur E, on trouve finalement

$$\mathbb{M}_{nr}(D) \cong \mathbb{M}_{ms}(E).$$

Le théorème de Wedderburn (1.40) permet de conclure que $D \cong E$ en tant que F-algèbres.

$\boxed{\Leftarrow}$ On a que $D \otimes_F \mathbb{M}_{nm}(F) \cong E \otimes_F \mathbb{M}_{nm}(F)$, d'où

$$\mathbb{M}_n(D) \otimes_F \mathbb{M}_m(F) \cong \mathbb{M}_m(E) \otimes_F \mathbb{M}_n(F),$$

i.e. $A \otimes_F \mathbb{M}_m(F) \cong B \otimes_F \mathbb{M}_n(F)$.

Partie (c) : Il existe $r, s \in \mathbb{N}$ tels que $N \otimes_F \mathbb{M}_r(F) \cong M \otimes_F \mathbb{M}_s(F)$, d'où

$$\mathbb{M}_r(N) \cong \mathbb{M}_s(M),$$

et par le théorème de Wedderburn (1.40), on a $N \cong M$ en tant que F-algèbres. □

3.6 Proposition. Si F est algébriquement clos, alors $\mathrm{Br}(F) = \{1\}$.

Preuve. Soit D un F-corps gauche central simple sur F de dimension finie. On choisit une base $(x_i)_{i=1,\ldots,n}$ de D en tant que F-espace vectoriel. Pour $i \in \{1, \ldots, n\}$, $F(x_i) = F$. En effet, $F(x_i)$ est une extension de corps de F (car $F = \mathcal{Z}(D)$), et est algébrique sur F (car de degré fini). On peut donc utiliser l'hypothèse F algébriquement clos.

Ainsi, on a

$$D = F(x_1, \ldots, x_n) = F.$$

Soit maintenant $[A] \in \mathrm{Br}(F)$. Comme A est centrale simple sur F, il existe un F-corps gauche D centrale simple sur F tel que $A \cong \mathbb{M}_n(D)$ pour un certain $n \in \mathbb{N}$. Or on sait que $D = F$, ainsi $[A] = 1_{\mathrm{Br}(F)}$. □

Extensions de Corps

Soient F et K deux corps tels que $F \subseteq K$, et A une F-algèbre. On donne une structure de K-algèbre à $A \otimes_F K$ en définissant le produit scalaire

$$k \cdot (a \otimes l) := (1 \otimes k)(a \otimes l) = a \otimes (kl), \quad \text{pour tout } k, l \in K \text{ et } a \in A.$$

3.7 Proposition. Soit $F \subseteq K$ deux corps et V un F-espace vectoriel. Alors

(a) à toute F-base $\{v_i \mid i \in I\}$ de V, on peut faire correspondre une K-base de $V \otimes_F K$

$$\{v_i \otimes 1 \mid i \in I\} ;$$

(b) en particulier, si $\dim_F(V) < \infty$, on a

$$\dim_K(V \otimes_F K) = \dim_F(V).$$

Preuve. On choisit une F-base $\{v_i \mid i \in I\}$ de V. Soit $x \in V \otimes_F K$ quelconque s'écrivant comme une somme de produits tensoriels d'éléments

de V et de K. En décomposant chaque élément de V dans la F-base des v_i, on trouve qu'il existe un nombre fini de scalaires $k_i \in K$ tels que

$$x = \sum_i v_i \otimes k_i,$$

ce qui montre que l'ensemble de vecteurs

$$\{v_i \otimes 1 \mid i \in I\}$$

engendre $V \otimes_F K$ par K-combinaisons linéaires. Il nous reste à voir qu'ils sont K-linéairement indépendants. Supposons qu'il existe un nombre fini de scalaires $\mu_i \in K$ tels que

$$\sum_i \mu_i (v_i \otimes 1) = 0.$$

On choisit alors $\{m_j \mid j \in J\}$ une F-base de K. Chaque coefficient μ_i se décompose dans cette base

$$\mu_i = \sum_j \mu_{ij} m_j$$

avec les μ_{ij} dans F et presque tous nuls pour tout i. Ainsi

$$\sum_i \left(\sum_j \mu_{ij} m_j \right) (v_i \otimes 1) = 0,$$

qu'on peut réécrire comme

$$\sum_j \left(\sum_i \mu_{ij} v_i \right) \otimes m_j = 0.$$

Par la F-indépendance linéaire des m_j, on a, par (2.10), que pour tout j

$$\sum_i \mu_{ij} v_i = 0.$$

Or les v_i forment une F-base de V, et donc $\mu_{ij} = 0$ pour tout i, j. Ce qui finit de démontrer (a) et (b) □

3.8 Corollaire. Soit $L_0 \subseteq L_1 \subseteq \cdots \subseteq L_N$ une suite de corps emboîtés, et A une L_0-algèbre. On note

$$A_N := (\cdots ((A \otimes_{L_0} L_1) \otimes_{L_1} L_2) \cdots) \otimes_{L_{N-1}} L_N.$$

Alors

(a) À toute L_0-base $\{a_i \mid i \in I\}$ de A, on peut faire correspondre une L_N-base de A_N

$$\{a_i \otimes \underbrace{1 \otimes \cdots \otimes 1}_{N \text{ fois}} \mid i \in I\} ;$$

(b) En particulier, si $\dim_{L_0}(A) < \infty$, on a

$$\dim_{L_N}(A_N) = \dim_{L_0}(A).$$

PREUVE. Immédiat de (3.7). □

3.9 Proposition. Soit F un corps et K une extension de F. Pour toute F-algèbre A, on a alors

(a) $A \otimes_F K$ est K-centrale si et seulement si A est F-centrale ;

(b) Si A est F-centrale alors : $A \otimes_F K$ est simple si et seulement si A est simple ;

(c) $A \otimes_F K$ est centrale simple sur K si et seulement si A est centrale simple sur F.

PREUVE. *Partie* (a) : $\boxed{\Rightarrow}$ On a que

$$K = \mathcal{Z}(A \otimes_F K) = \mathcal{Z}(A) \otimes_F \mathcal{Z}(K) = \mathcal{Z}(A) \otimes_F K.$$

Or $\dim_K(K) = 1$ et, par (3.7), $\dim_K(\mathcal{Z}(A) \otimes_F K) = \dim_F(\mathcal{Z}(A))$, ainsi $\dim_F(\mathcal{Z}(A)) = 1$, *i.e.* $\mathcal{Z}(A) = F$.

$\boxed{\Leftarrow}$ On a que

$$\mathcal{Z}(A \otimes_F K) = \mathcal{Z}(A) \otimes_F \mathcal{Z}(K) = F \otimes_F K.$$

On a déjà vu que $F \otimes_F K \cong K$ en tant que F-espaces vectoriels. Pour voir qu'on a $F \otimes_F K \cong K$ en tant que K-espaces vectoriels (et pouvoir alors conclure par (1.5)), on remarque que $\dim_K(F \otimes_F K) = \dim_F(F) = 1$, par (3.7).

Partie (b) : $\boxed{\Rightarrow}$ Par contraposition, on suppose que A n'est pas simple, *i.e.* A possède un idéal propre I. On peut vérifier que $I \otimes_F K$ est un idéal de $A \otimes_F K$. Cet idéal est non-zéro comme $\dim_K(I \otimes_F K) = \dim_F(I) > 0$. De plus,

$$\dim_K(A \otimes_F K) = \dim_F(A) > \dim_F(I) = \dim_K(I \otimes_F K),$$

ce qui montre que $I \otimes_F K$ est idéal propre de $A \otimes_F K$ qui n'est donc pas simple.

$\boxed{\Leftarrow}$ Démontré en (2.13).

Partie (c) : Découle de (a) et (b). □

3.10 Lemme. Soit F, K deux corps tels que $F \subseteq K$ et A, B deux F-algèbres. Alors

$$A \cong B \quad \Longrightarrow \quad A \otimes_F K \cong B \otimes_F K,$$

où le premier isomorphisme est un isomorphisme de F-algèbres, et le second de K-algèbres.

PREUVE. On a un isomorphisme $\pi : A \to B$ de F-algèbres. On définit alors avec une F-base $\{a_i \mid i \in I\}$ de A un isomorphisme de K-espaces vectoriels avec les éléments de la K-base $\{a_i \otimes 1 \mid i \in I\}$ de $A \otimes_F K$

$$\varphi : A \otimes_F K \longrightarrow B \otimes_F K, \quad a_i \otimes 1 \longmapsto \pi(a_i) \otimes 1,$$

et on peut vérifier qu'il s'agit d'un isomorphisme de K-algèbres. □

3.11 Lemme. Soit F, K deux corps tels que $F \subseteq K$, A une F-algèbre et n un entier. Alors on a les isomorphismes de K-algèbres

(a) $\mathbb{M}_n(A) \otimes_F K \cong \mathbb{M}_n(A \otimes_F K)$;

(b) $(\mathbb{M}_n(F) \otimes_F A) \otimes_F K \cong \mathbb{M}_n(A \otimes_F K)$.

PREUVE. *Partie* (a) : On choisit $\{a_i \mid i \in I\}$ une F-base de A avec laquelle on construit une K-base de $\mathbb{M}_n(A) \otimes_F K$, en utilisant les notations de (1.17),

$$\{(a_i E_{rs}) \otimes 1 \mid i \in I \text{ et } r, s = 1, \ldots, n \}.$$

On définit avec les éléments de cette base un isomorphisme de K-espaces vectoriels

$$\varphi : \mathbb{M}_n(A) \otimes_F K \longrightarrow \mathbb{M}_n(A \otimes_F K), \quad (a_i E_{rs}) \otimes 1 \longmapsto E_{rs}(a_i \otimes 1).$$

La bijecivité de φ est immédiate comme les $E_{rs}(a_i \otimes 1)$ avec $i \in I$ et $r, s = 1, \ldots, n$ forment une K-base de $\mathbb{M}_n(A \otimes_F K)$.

On vérifie de plus que φ est bien un homomorphisme de K-algèbres.

Partie (b) : On sait déjà que $\mathbb{M}_n(F) \otimes_F A \cong \mathbb{M}_n(A)$ en tant que F-algèbres. Par (3.10), on a alors que $(\mathbb{M}_n(F) \otimes_F A) \otimes_F K \cong \mathbb{M}_n(A) \otimes_F K$ en tant que K-algèbres, et avec (a) on peut conclure. □

3.12 Proposition. Soit F, K deux corps tels que $F \subseteq K$. Alors

(a) l'application

$$r_{K/F} : \mathrm{Br}(F) \longrightarrow \mathrm{Br}(K), \quad [A] \longmapsto [A \otimes_F K]$$

est un homomorphisme de groupes bien défini ;

(b) si L est un corps avec $F \subseteq K \subseteq L$, alors

$$r_{L/F} = r_{L/K} \circ r_{K/F}.$$

PREUVE. *Partie* (a) :

– *Bien défini* : Nous savons par (3.9) que $[A \otimes_F K] \in \mathrm{Br}(K)$ pour tout $[A] \in \mathrm{Br}(F)$.
Soit A, B deux F-algèbres centrales simples sur F et membres de la même classe d'équivalence dans $\mathrm{Br}(F)$, *i.e.* il existe n, m des entiers tels que

$$A \otimes_F \mathbb{M}_n(F) \cong B \otimes_F \mathbb{M}_m(F),$$

en tant que F-algèbres. Par (3.10), on a l'isomorphisme de K-algèbres

$$(A \otimes_F \mathbb{M}_n(F)) \otimes_F K \cong (B \otimes_F \mathbb{M}_m(F)) \otimes_F K,$$

et par (b) de (3.11), on a alors l'isomorphisme de K-algèbres

$$\mathbb{M}_n(A \otimes_F K) \cong \mathbb{M}_m(B \otimes_F K).$$

– *Homomorphisme de groupe* : Pour $[A], [B] \in \mathrm{Br}(F)$

$$\begin{aligned} r_{K/F}([A] \cdot [B]) &= [(A \otimes_F B) \otimes_F K] \quad \text{et} \\ r_{K/F}[A] \cdot r_{K/F}[B] &= [(A \otimes_F K) \otimes_K (B \otimes_F K)]. \end{aligned}$$

Nous allons construire un isomorphisme de K-algèbres de $(A \otimes_F B) \otimes_F K$ à $(A \otimes_F K) \otimes_K (B \otimes_F K)$. Premièrement, on prend $\{a_i \mid i \in I\}$ une F-base de A et $\{b_j \mid j \in J\}$ une F-base de B, ce qui nous permet de construire des K-bases de $(A \otimes_F B) \otimes_F K$ et de $(A \otimes_F K) \otimes_K (B \otimes_F K)$

$$\{(a_i \otimes b_j) \otimes 1 \mid i \in I, j \in J\} \quad \text{et} \quad \{(a_i \otimes 1) \otimes (b_j \otimes 1) \mid i \in I, j \in J\}.$$

On définit alors un isomorphisme de K-espaces vectoriels par

$$\begin{array}{rccc} \varphi : & (A \otimes_F B) \otimes_F K & \longrightarrow & (A \otimes_F K) \otimes_K (B \otimes_F K) \\ & (a_i \otimes b_j) \otimes 1 & \longmapsto & (a_i \otimes 1) \otimes (b_j \otimes 1), \end{array}$$

et on vérifie qu'il s'agit aussi d'un isomorphisme de K-algèbres.

Partie (b) : Soit $[A] \in \mathrm{Br}(F)$, on doit voir que $r_{L/F}[A] = (r_{L/K} \circ r_{K/F})[A]$, *i.e.*

$$[A \otimes_F L] = [(A \otimes_F K) \otimes_K L].$$

Nous allons montrer que $A \otimes_F L \cong (A \otimes_F K) \otimes_K L$ en tant que L-algèbres. On commence par prendre $\{a_i \mid i \in I\}$ une F-base de A , ce qui nous permet de construire des L-bases de $A \otimes_F L$ et de $(A \otimes_F K) \otimes_K L$

$$\{a_i \otimes 1 \mid i \in I\} \quad \text{et} \quad \{(a_i \otimes 1) \otimes 1 \mid i \in I\},$$

on définit alors un isomorphisme de L-espaces vectoriels par

$$\begin{array}{rccc} \varphi : & A \otimes_F L & \longrightarrow & (A \otimes_F K) \otimes_K L \\ & a_i \otimes 1 & \longmapsto & (a_i \otimes 1) \otimes 1, \end{array}$$

et on vérifie qu'il s'agit aussi d'une isomorphisme de L-algèbres. □

3.13 Caractérisation des algèbres centrales simples. Soit A une algèbre de dimension finie sur un corps F et $\overline{F}$ une clôture algébrique de F. Alors les conditions suivantes sont équivalentes :

(i) A est centrale simple sur F ;

(ii) il existe un F-corps gauche D central simple sur F tel que $A \cong \mathbb{M}_n(D)$ en tant que F-algèbres, pour un certain entier n ;

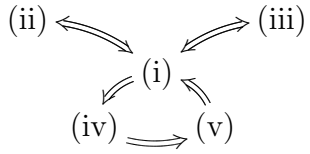
(iii) il existe un isomorphisme de F-algèbres

$$A \otimes_F A^{\mathrm{op}} \longrightarrow \mathrm{End}_F(A), \quad (a, b) \longmapsto (x \mapsto axb) \ ;$$

(iv) il existe un isomorphisme de $\overline{F}$-algèbres $A \otimes_F \overline{F} \cong \mathbb{M}_n(\overline{F})$ pour un certain entier n ;

(v) il existe une extension de corps K de F telle que $A \otimes_F K \cong \mathbb{M}_n(K)$ en tant que K-algèbres, pour un certain entier n.

Preuve.



"(i) ⇒ (ii)" Vu en (3.5).

"(ii) ⇒ (i)" Par (1.19) et (1.21).

"(i) ⇒ (iii)" Vu en (3.2).

"(iii) ⇒ (i)" On sait par (1.29) que $\mathrm{End}_F(A) \cong \mathbb{M}_n(F)$ en tant que F-algèbres pour un certain entier n, et on a déjà vu que $\mathbb{M}_n(F)$ est centrale simple sur F. Pour voir que A est F-central, on remarque que

$$1 = \dim_F(\mathcal{Z}(\mathbb{M}_n(F))) = \dim_F(\mathcal{Z}(A) \otimes_F \mathcal{Z}(A^{\mathrm{op}})) = \dim_F(\mathcal{Z}(A))^2.$$

Pour voir que A est simple, on procède par contraposition. Si A n'est pas simple, alors il existe un idéal propre I de A. On peut vérifier que $I \otimes_F A^{\mathrm{op}}$ est un idéal de $A \otimes_F A^{\mathrm{op}}$, on alors avec

$$\dim_F(I \otimes_F A^{\mathrm{op}}) = \dim_F(I) \cdot \dim_F(A^{\mathrm{op}})$$

et $0 < \dim_F(I) < \dim_F(A)$, que $I \otimes_F A^{\mathrm{op}}$ est un idéal propre de $A \otimes_F A^{\mathrm{op}}$ qui n'est donc pas simple.

"(i) $\Rightarrow$ (iv)" Par (3.9), $A \otimes_F \overline{F}$ est centrale simple sur $\overline{F}$, *i.e.* $A \otimes_F \overline{F} \in \mathrm{Br}(\overline{F})$. Avec (3.6), on peut conclure.

"(iv) $\Rightarrow$ (v)" Immédiat.

"(v) $\Rightarrow$ (i)" On sait que $\mathbb{M}_n(K)$ est centrale simple sur K, on peut donc utiliser (3.9). □

3.14 Définition. Soit F un corps et A une F-algèbre centrale simple sur F. On sait par Wedderbrun (1.40) qu'il existe un (unique) entier n et un (unique à isomorphismes de F-algèbres près) F-corps gauche D tels que $A \cong \mathbb{M}_n(D)$ en tant que F-algèbre. On définit le **degré** de A par

$$\deg_F(A) := \sqrt{\dim_F(A)},$$

et l'**indice** de A par

$$\mathrm{ind}_F(A) := \sqrt{\dim_F(D)}.$$

En particulier

$$\mathrm{ind}_F(A) = \deg_F(D).$$

(On sait par (3.5) que D est central simple sur F.)

3.15 Proposition. Soit F un corps et A une F-algèbre (de dimension finie) centrale simple sur F. Alors

(a) $\deg_F(A)$ et $\mathrm{ind}_F(A)$ sont des entiers ;

(b) $\mathrm{ind}_F(A)$ divise $\deg_F(A)$;

(c) pour tout F-corps gauche C centrale sur F, $\dim_F(C)$ est un carré ou ∞.

Preuve. *Partie* (a) : Il suffit de montrer que $\deg_F(A)$ est entier. Par (3.13), il existe une extension K de F telle que $A \otimes_F K \cong \mathbb{M}_m(K)$ pour un certain entier m. Ainsi, avec (3.7),

$$\dim_F(A) = \dim_K(A \otimes_F K) = \dim_K(\mathbb{M}_m(K)) = m^2,$$

ce qui montre que $\deg_F(A)$ est entier.

Partie (b) : Soit D un F-corps gauche central simple sur F tel que $A \cong \mathbb{M}_n(D)$, pour un certain entier n. On a

$$\dim_F(A) = \dim_F(\mathbb{M}_n(D)) = \dim_F(D) \cdot n^2,$$

et en prenant la racine des deux côtés, on peut conclure.

Partie (c) : Tout corps gauche est simple, ainsi si C est un F-corps gauche de dimension finie et de centre F, alors $[C] \in \mathrm{Br}(F)$. Par (a), $\dim_F(C)$ est un carré. □

Chapitre 4

Quaternions

Formes Quadratiques

Dans cette section, nous introduisons les concepts de base liés aux formes quadratiques qui nous seront utiles dans la section suivante sur les quaternions. Comme les formes quadratiques ne sont pas le thème de ce projet, le matériel présenté ici est abrégé et presque rien n'est justifié. Pour des meilleures introductions, on pourra se référer aux deux livres qui ont servi à écrire cette section : [3, p. 1-12, 19-24] et [4, p. 1-15].

Pour toute cette section, F désigne un corps de caractéristique différente de 2. On note $\dot{F} = F \setminus \{0\}$ le groupe multiplicatif de F.

4.1 Définition. Une **forme quadratique** (n-aire) sur F est un polynôme f en n variables sur F homogène de degré 2, *i.e.* f est de la forme

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \in F[X_1, \ldots, X_n],$$

avec $a_{ij} \in F$ pour $i, j = 1, \ldots n$.

En notant X le vecteur colonne avec composantes $X_1, \ldots, X_n$ et M_f la matrice des a_{ij}, on écrit f comme

$$f(X) = X^t \cdot M_f \cdot X.$$

La matrice M_f n'est pas nécessairement unique. Cependant, il existe une unique matrice *symétrique* représentant f. On peut la construire à partir d'une représentation M_f quelconque de f en utilisant l'équation

$$\left(M_f^{\text{sym}}\right)_{ij} = \frac{1}{2}\left((M_f)_{ij} + (M_f)_{ji}\right).$$

Par la suite, on supposera toujours que la matrice M_f représentant f est symétrique (et ainsi unique).

4.2 Définition. Deux formes quadratiques n-aires f et g sont dites **équivalentes** s'il existe une matrice inversible $C \in \mathrm{GL}_n(F)$ telle que

$$f(X) = g(C \cdot X),$$

on note alors $f \cong g$.

Il est facile de vérifier que "$\cong$" est bien une relation d'équivalence, en utilisant, par exemple, que $f \cong g$ équivaut à $M_f = C^t \cdot M_g \cdot C$ pour un certain $C \in \mathrm{GL}_n(F)$

4.3 Définition. Soit f une forme quadratique n-aire. On définit l'**application quadratique** $Q_f : F^n \to F$ **associée à** f par

$$Q_f(x) := f(x) = x^t \cdot M_f \cdot x,$$

pour tout vecteur colonne $x \in F^n$.

L'application Q_f est "quadratique" dans le sens où

$$Q_f(ax) = a^2 Q_f(x), \quad \text{pour tout } a \in F \text{ et } x \in F^n.$$

La forme quadratique f détermine Q_f, et réciproquement on peut retrouver f à partie de Q_f en utilisant les formules

$$\begin{aligned} Q_f(e_i) &= (M_f)_{ii}\,, \\ Q_f(e_i + e_j) &= (M_f)_{ii} + (M_f)_{jj} + 2\,(M_f)_{ij}\,, \end{aligned}$$

où e_i et e_j sont des vecteurs de base standards de F^n. (Ici nous utilisons pour la *deuxième* fois l'hypothèse que la caractéristique de F est différente de 2).

4.4 Définition. Soit f une forme quadratique n-aire et Q_f l'application quadratique associée. On définit la **forme symétrique bilinéaire associée à** f

$$B_f : F^n \times F^n \longrightarrow F$$

par

$$B_f(x, y) = \frac{1}{2}(Q_f(x + y) - Q_f(x) - Q_f(y)).$$

On peut facilement vérifier l'égalité

$$B_f(x, y) = x^t \cdot M_f \cdot y,$$

d'où on voit que B_f est bien une forme bilinéaire (sa symétrie étant directe à partir de sa définition).

La dernière équation implique également qu'on peut retrouver Q_f à partir de B_f, comme on a

$$B_f(x, x) = Q_f(x).$$

4.5 Définition. Soit V un F-espace vectoriel de dimension finie. Une application $Q : V \to F$ est dite **application quadratique** si elle satisfait les conditions

(a) $Q(av) = a^2 Q(v)$, pour tout $a \in F$ et $v \in V$,

(b) l'application $B : V \times V \to F$ définie par

$$B(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)), \quad \text{pour tout } x, y \in V,$$

est F-bilinéaire (et symétrique).

Ainsi toute application quadratique $Q : V \to F$ engendre une forme bilinéaire symétrique.

Réciproquement, toute forme bilinéaire symétrique $B : V \times V \to F$ engendre une application quadratique $q_B : V \to F$ définie par l'équation

$$q_B(x) = B(x, x), \quad \text{pour tout } x \in V.$$

De plus, les deux opérations sont l'inverse l'une de l'autre. (On pourrait parler de "polarisation" et de "dépolarisation").

4.6 Définition. Soit V un F-espace vectoriel de dimension finie, et $B : V \times V \to F$ une forme bilinéaire symétrique. On dit alors que le couple (V, B) est un **espace quadratique**, avec pour **application quadratique associée** $q_B : V \to F$ définie par

$$q_B(x) = B(x, x).$$

Comme nous avons vu ci-dessus, la donnée d'une forme bilinéaire symétrique ou de sa forme quadratique associée est équivalente. Dès lors, on pourra noter les espaces quadratiques sous la forme (V, B) ou (V, q_B).

On remarque que, pour toute forme quadratique n-aire f, $(F^n, B_f) = (F^n, Q_f)$ est un espace quadratique. On le notera parfois aussi (F^n, f).

Réciproquement, tout espace quadratique (V, B) engendre, à partir de tout choix de F-base $\{v_1, \ldots, v_n\}$, une forme quadratique f définie par

$$f(X_1, \ldots, X_n) := \sum_{i,j=1}^{n} B(v_i, v_j) X_i X_j,$$

telle que pour tout $x \in V$

$$q_B(x) = f(D(x)),$$

où $D : V \to F^n$ est l'opérateur de décomposition dans la base $\{v_1, \ldots, v_n\}$.

La forme quadratique f engendrée par l'espace quadratique (V, B) n'est pas unique, mais déterminée à équivalence de forme quadratique près.

On peut voir cela en choisissant une autre F-base $\{w_1, \ldots, w_n\}$ de V s'écrivant comme

$$w_i = \sum_{k=1}^{n} \lambda_{ki} \cdot v_k,$$

avec $\lambda_{ki} \in F$, et générant donc la forme quadratique

$$f'(X_1, \ldots, X_n) := \sum_{i,j=1}^{n} B(w_i, w_j) X_i X_j.$$

On a alors

$$\begin{aligned}(M_{f'})_{ij} = B(w_i, w_j) &= \sum_{k,l=1}^{n} B(\lambda_{ki} \cdot v_k, \lambda_{lj} \cdot v_l) \\ &= \sum_{k,l=1}^{n} \lambda_{ki} \cdot B(v_k, v_l) \cdot \lambda_{lj} = \left(\Lambda^t \cdot M_f \cdot \Lambda\right)_{ij},\end{aligned}$$

où $\Lambda = (\lambda_{kl}) \in \mathrm{GL}_n(F)$. On a donc bien que $f \cong f'$.

Réciproquement, on voit par le calcul que nous venons de faire que pour tout forme quadratique $\widetilde{f}$ avec $\widetilde{f} \cong f$, on peut trouver une F-base de V telle que la forme quadratique associée soit précisément $\widetilde{f}$.

Ainsi, (V, B) détermine une classe dans la relation d'équivalence de formes quadratiques, on la notera par (f_B).

On définit maintenant une relation d'équivalence sur les espaces quadratiques qui corresponde précisément à l'équivalence des formes quadratiques :

4.7 Définition. On dit que deux espaces quadratiques (V, B) et (V', B') sont **isométriques** s'il existe un isomorphisme de F-espaces vectoriels $\tau : V \to V'$ tel que

$$B'(\tau(x), \tau(y)) = B(x, y), \quad \text{pour tout } x, y \in V.$$

Dans ce cas, on note

$$(V, B) \cong (V', B').$$

On peut montrer que

$$(V, B) \cong (V', B') \quad \Longleftrightarrow \quad (f_B) = (f_{B'}).$$

Une condition équivalente pour $(V, B) \cong (V', B')$ est qu'il existe un isomorphisme de F-espaces vectoriels $\varphi : V \to V'$ tel que

$$Q_{B'}(\varphi(x)) = Q_B(x), \quad \text{pour tout } x \in V,$$

On note que si l'espace quadratique (V, B) engendre une forme quadratique f, alors $(V, B) \cong (F^n, B_f)$.

Dès lors, comme la classe d'équivalence de f permet de déterminer la classe d'équivalence de (V, B) et inversément, on pourra, si on travaille à équivalence près, passer librement des espaces quadratiques aux formes quadratiques et inversément.

4.8 Définition. Soit $d \in \dot{F} = F \setminus \{0\}$ et (V, B) un espace quadratique avec application quadratique associée q_B. On dit que q_B **représente** d s'il existe $v \in V$ tel que

$$q_B(v) = d.$$

On note $D(q_B)$ l'ensemble des valeurs dans $\dot{F}$ représentées par q_B.

S'il n'y a pas d'ambiguïté sur la forme bilinéaire B, on notera parfois $D(V)$ à la place de $D(q_B)$.

Il est facile de voir que $D(q_B)$ dépend uniquement de la classe d'équivalence de (V, B). Ainsi, si (V, q_B) engendre sur F^n une forme quadratique f, alors on a que $D(q_B) = D(Q_f)$.

Soit (V_1, B_1) et (V_2, B_2) deux espaces quadratiques. On définit sur $V = V_1 \oplus V_2$ une nouvelle forme bilinéaire symétrique $B : V \times V \to F$ par

$$B((x_1, x_2), (y_1, y_2)) := B_1(x_1, y_1) + B(x_2, y_2).$$

On peut vérifier que (V, B) ainsi défini est bien un espace quadratique qui a la propriété

$$B(V_1, V_2) = B(V_2, V_1) = \{0\}.$$

4.9 Définition. On appelle l'espace quadratique (V, B) défini ci-dessus la **somme orthogonale** de (V_1, B_1) et (V_2, B_2), et on le note $V_1 \perp V_2$.

Il est clair que si V_1, V_2 et V_1', V_2' sont quatre espaces quadratiques tels que $V_1 \cong V_1'$ et $V_2 \cong V_2'$, alors

$$V_1 \perp V_2 \cong V_1' \perp V_2'.$$

Pour $d \in F$, on note par $\langle d \rangle$ l'espace quadratique (F, q) avec q défini par

$$q(x) = dx^2, \quad \text{pour tout } x \in F.$$

4.10 Critère de Représentation. Soit (V, B) un espace quadratique.

(a) Si $d \in D(V)$, alors il existe un espace quadratique (V', B') tel que

$$V \cong \langle d \rangle \perp V'.$$

(b) Il existe $d_1, \ldots, d_n \in F$ tels que

$$V \cong \langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle.$$

Pour simplifier on notera $\langle d_1, \ldots, d_n \rangle$ à la place de $\langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle$.

La partie (b) implique que tout espace quadratique engendre une forme quadratique représentée par une matrice diagonale (avec pour coefficients sur la diagonale $d_1, \ldots, d_n$).

4.11 Règles de calcul. Soient $a, b \in F$ et $c, d \in \dot{F}$, alors

$$\langle a, b \rangle \cong \langle b, a \rangle$$
$$\langle a, b \rangle \cong \langle ac^2, bd^2 \rangle$$

4.12 Définition. Soit f une forme quadratique représentée par la matrice (symétrique) M_f, on définit le **déterminant** de f dans $\dot{F}/\dot{F}^2$ par

$$d(f) := \det(M_f) \cdot \dot{F}^2.$$

On peut vérifier que si $f \cong g$, alors $d(f) = d(g)$ dans $\dot{F}/\dot{F}^2$.

On étend naturellement la définition de déterminant aux espaces quadratiques en définissant le déterminant $d(V)$ d'un espace quadratique (V, B) comme $d(f)$, où f est une forme quadratique engendrée par (V, B) (on a montré ci-dessus qu'elle sont toutes équivalentes).

L'espace quadratique (V, B) est dit **régulier** si son déterminant $d(V)$ est non-zéro.

Une observation immédiate est que si $(V, B) \cong \langle d_1, \ldots, d_n \rangle$, alors

$$d(V) = d_1 \cdots d_n \cdot \dot{F}^2.$$

4.13 Définition. Soit v un vecteur non-zéro dans un espace quadratique (V, B). On dit que v est **isotrope** si $B(v, v) = 0$, sinon v est dit **anisotrope**.

L'espace quadratique (V, B) est dit **isotrope** s'il contient un vecteur (non-zéro) isotrope, sinon l'espace quadratique est dit **anisotrope**.

4.14 Proposition. Soit (V, B) est un espace quadratique régulier et isotrope avec $\dim_F(V) \geq 2$. Alors il existe un espace quadratique (V', B') tel que

$$V \cong \langle -1, 1 \rangle \perp V'.$$

On dit que l'espace quadratique $\langle -1, 1\rangle$ est le **plan hyperbolique**. Un espace quadratique isométrique à une somme orthogonale de plans hyperboliques est appelé **espace hyperbolique**.

4.15 Théorème d'Annulation de Witt. Pour V, W et W' trois espaces quadratiques, on a l'implication

$$V \perp W \cong V \perp W' \quad \Longrightarrow \quad W \cong W'.$$

Algèbres des Quaternions

Les démonstrations présentées dans cette section sont tirées de [3, p. 74-78] et [4, p. 51-61].

Fixons pour toute cette section un corps F de caractéristique différente de 2 et $a, b \in \dot{F} = F \setminus \{0\}$.

Nous allons construire l'algèbre des quaternions $\left(\frac{a,b}{F}\right)$ comme une sous-F-algèbre de $\mathbb{M}_2(E)$, où E est une clôture algébrique de F.

On commence par choisir α et β dans E tels que

$$\alpha^2 = -a \quad \text{et} \quad \beta^2 = b,$$

pour pouvoir définir

$$i := \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} \quad \text{et} \quad j := \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}.$$

On vérifie par des calculs directs que

$$i^2 = a \cdot \mathbb{1}_2, \quad j^2 = b \cdot \mathbb{1}_2, \quad k := ij = \begin{pmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{pmatrix}, \quad \text{et} \quad ij = -ji.$$

En utilisant tout ceci, on déduit facilement la table de multiplication suivante (à lire dans le sens "ligne multiplie colonne").

$\cdot$	i	j	k
i	a	k	aj
j	$-k$	b	$-bi$
k	$-aj$	bi	$-ab$

En particulier, i, j, k anticommutent deux-à-deux. On note par $\left(\frac{a,b}{F}\right)$ le F-espace vectoriel engendré par F-combinaisons linéaires de $\{1, i, j, k\}$ (où $1 = \mathbb{1}_2$).

Comme $\{1, i, j, k\}$ engendrent (clairement) par E-combinaisons linéaires le E-espace vectoriel $\mathbb{M}_2(E)$ (qui est de E-dimension 4), on a nécessairement que $\{1, i, j, k\}$ sont E-linéairement indépendants. Ils sont donc aussi F-linéairement indépendants. De là, on déduit qu'ils forment une F-base de $\left(\frac{a,b}{F}\right)$, qui est donc de F-dimension 4.

En examinant la table de multiplication ci-dessus, on constate que les éléments de $\left(\frac{a,b}{F}\right)$ sont stables par multiplication matricielle. En munissant $\left(\frac{a,b}{F}\right)$ du produit matriciel standard, on lui donne donc un structure de F-algèbre.

Enfin, il est clair qu'à isomorphisme de F-algèbres près la construction de $\left(\frac{a,b}{F}\right)$ est indépendante du choix des racines α et β.

4.16 Définition. On appelle l'algèbre $\left(\frac{a,b}{F}\right)$ construite ci-dessus l'**algèbre des quaternions** de a, b sur F.

On dira parfois que $\{1, i, j, k\}$ est la base "standard" de $\left(\frac{a,b}{F}\right)$.

4.17 Exemple. Dans le cas de $\left(\frac{-1,1}{F}\right)$, on peut choisir comme racines

$$\alpha = 1 \quad \text{et} \quad \beta = 1,$$

il apparaît ainsi que, dans ce cas, l'ensemble $\{1, i, j, k\}$ forme en fait une F-base de $\mathbb{M}_2(F)$, et donc

$$\left(\frac{-1,1}{F}\right) = \mathbb{M}_2(F). \tag{4.18}$$

4.19 Remarque. On peut facilement construire un isomorphisme de $\mathbb{R}$-algèbres entre $\left(\frac{-1,-1}{\mathbb{R}}\right)$ et le corps gauche de Hamilton $\mathbb{H}$ défini dans la section "Algèbre de Hamilton" du chapitre 1.

4.20 Proposition. Si K est un extension de corps de F, alors

$$K \otimes_F \left(\frac{a,b}{F}\right) \cong \left(\frac{a,b}{K}\right), \quad \text{comme } K\text{-algèbres.}$$

Preuve. Soit $\{1, i, j, k\}$ et $\{1, i', j', k'\}$ les bases standards de $\left(\frac{a,b}{F}\right)$ et $\left(\frac{a,b}{K}\right)$.

On construit une K-base de $K \otimes_F \left(\frac{a,b}{F}\right)$:

$$\{\, 1 \otimes 1,\ 1 \otimes i,\ 1 \otimes j,\ 1 \otimes k \,\}.$$

Ce qui nous permet de définir un isomorphisme de K-espaces vectoriels

$$\varphi :\ K \otimes_F \left(\frac{a,b}{F}\right) \longrightarrow \left(\frac{a,b}{K}\right),$$

par

$$\varphi(1 \otimes 1) = 1, \;\; \varphi(1 \otimes i) = i', \;\; \varphi(1 \otimes j) = j', \;\; \varphi(1 \otimes k) = k'.$$

On peut facilement vérifier qu'il s'agit d'un isomorphisme de K-algèbres. □

La proposition précédente nous permet d'obtenir le résultat suivant, qui relie aux groupes de Brauer l'algèbre des quaternions.

4.21 Proposition. La F-algèbre $\left(\frac{a,b}{F}\right)$ est centrale simple sur F.

PREUVE. Soit E une clôture algébrique de F. Par la proposition précédente, on sait que

$$E \otimes_F \left(\frac{a,b}{F}\right) \cong \left(\frac{a,b}{E}\right).$$

Comme $\left(\frac{a,b}{E}\right)$ est une E-sous-algèbre de $\mathbb{M}_2(E)$ de dimension 4, on a nécessairement

$$\left(\frac{a,b}{E}\right) = \mathbb{M}_2(E).$$

Ainsi, comme $\mathbb{M}_2(E)$ est simple, on a $E \otimes_F \left(\frac{a,b}{F}\right)$ simple. D'où on déduit que $\left(\frac{a,b}{F}\right)$ est simple.

De plus,

$$\mathcal{Z}(E) \otimes_F \mathcal{Z}\left(\frac{a,b}{F}\right) = \mathcal{Z}\left(E \otimes_F \left(\frac{a,b}{F}\right)\right) = \mathcal{Z}(\mathbb{M}_2(E)) = E,$$

d'où

$$1 = \dim_E \left(\mathcal{Z}(E) \otimes_F \mathcal{Z}\left(\frac{a,b}{F}\right)\right) = \dim_F \left(\mathcal{Z}\left(\frac{a,b}{F}\right)\right).$$

□

4.22 Définition. Soit $x \in \left(\frac{a,b}{F}\right)$ s'écrivant comme

$$x = \alpha + \beta i + \gamma j + \delta k, \quad \text{avec } \alpha, \beta, \gamma, \delta \text{ dans } F.$$

On définit le **conjugué** de x

$$\overline{x} := \alpha - (\beta i + \gamma j + \delta k).$$

4.23 Proposition. Soit $x, y \in \left(\frac{a,b}{F}\right)$ et $r \in F$. On a les égalités suivantes

$$\overline{x+y} = \overline{x} + \overline{y}, \quad \overline{xy} = \overline{y}\,\overline{x}, \quad \overline{\overline{x}} = x, \quad \overline{rx} = r\overline{x},$$

i.e. l'opération de conjugaison est une involution.

PREUVE. La seule partie non-évidente est $\overline{xy} = \overline{y}\,\overline{x}$. Comme la conjugaison est linéaire, il suffit de le vérifier sur les vecteurs de base $1, i, j, k$. Par exemple, on a

$$\overline{ij} = \overline{k} = -k = -ij = ji = (-j)(-i) = \overline{j}\,\overline{i}.$$

Les autres vérifications sont similaires. □

Notons jusqu'à la fin de cette section $A := \left(\frac{a,b}{F}\right)$.

4.24 Définition. On définit le sous-F-espace vectoriel des **quaternions purs** $A_0 \subseteq A$ par

$$A_0 := \{x \in A \mid x = -\overline{x}\}.$$

Ce qui peut aussi être défini comme

$$A_0 = \{\beta i + \gamma j + \delta k \in A \mid \beta, \gamma, \delta \in F\}.$$

Nous avons la caractérisation suivante des quaternions purs, qui nous servira à démontrer le théorème (4.29).

4.25 Proposition. Si $v \in A \setminus \{0\}$, alors

$$v \in A_0 \quad \Longleftrightarrow \quad v \notin F \text{ et } v^2 \in F.$$

PREUVE. Notons $v = \alpha + \beta i + \gamma j + \delta k$ avec $\alpha, \beta, \gamma, \delta$ dans F. Un calcul direct montre que

$$v^2 = (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha(\beta i + \gamma j + \delta k).$$

Ainsi, on voit directement que si v est pur, alors $v^2 \in F$. Réciproquement, si $v \notin F$ (*i.e.* β, γ ou δ est non-zéro) et $v^2 \in F$, alors $\alpha = 0$. □

4.26 Remarque. Une conséquence de (4.25) est que A_0 est indépendant du choix de la base. En ce sens, on a une décomposition canonique

$$A \cong (F \cdot 1) \oplus A_0,$$

comme tout quaternion se décompose de manière unique en une partie scalaire dans F et une partie pure dans A_0.

Soit $x \in \left(\frac{a,b}{F}\right)$ se décomposant en $x = x_1 + x_0$ avec $x_1 \in F \cdot 1$ et $x_0 \in A_0$. On a

$$x\overline{x} = (x_1 + x_0)(x_1 - x_0) = x_1^2 - x_1x_0 + x_0x_1 - x_0^2 = x_1^2 - x_0^2$$

Ainsi, $x\overline{x} \in F$ (comme, par la proposition précédente, $x_0^2 \in F$).

4.27 Définition. L'application $N : A \to F$ qui à $x \in A$ associe $x\overline{x}$ est appelée la **norme** de A.

Pour tout $x, y \in \left(\frac{a,b}{F}\right)$, on a $N(xy) = N(x)N(y)$. En effet,

$$N(xy) = xy\overline{xy} = xy\overline{y}\,\overline{x} = xN(y)\overline{x} = N(x)N(y).$$

4.28 Proposition. (A, N) est un espace quadratique.

Preuve. Il faut vérifier que

(1) $N(ax) = a^2N(x)$ pour tout $a \in F$ et $x \in A$, et que

(2) l'application

$$B : A \times A \longrightarrow F, \quad (x, y) \longmapsto \frac{1}{2}(N(x + y) - N(x) - N(y))$$

est F-bilinéaire.

La partie (1) est immédiate. Pour la partie (2), on calcule que pour $x, y \in A$ quelconques :

$$\begin{aligned} B(x, y) = \frac{1}{2}(N(x + y) - N(x) - N(y)) &= \frac{1}{2}\left((x + y)\overline{(x + y)} - x\overline{x} - y\overline{y}\right) \\ = \frac{1}{2}(x\overline{x} + x\overline{y} + y\overline{x} + y\overline{y} - x\overline{x} - y\overline{y}) &= \frac{1}{2}(x\overline{y} + y\overline{x}), \end{aligned}$$

d'où on peut assez facilement déduire la F-bilinéarité. □

En reprenant le calcul fait dans la dernière démonstration, on constate que

(a) si x est pur et $y = 1$, alors

$$B(x, 1) = \frac{1}{2}(x - x) = 0,$$

(b) si x et y sont purs, alors

$$B(x, y) = -\frac{1}{2}(xy + yx).$$

Ainsi, comme i, j, k anticommutent, les vecteurs $\{1, i, j, k\}$ forment une base orthogonale du F-espace quadratique (A, N). De plus, on calcule

$$N(1) = 1\overline{1} = 1, \quad N(i) = i\overline{i} = -i^2 = -a, \quad N(j) = j\overline{j} = -j^2 = -b$$
$$N(k) = k\overline{k} = -k^2 = ab.$$

De cela, on déduit que la décomposition dans la F-base orthogonale $\{1, i, j, k\}$ est un isométrie naturelle entre (A, N) et $(F^4, \langle 1, -a, -b, ab\rangle)$.

Pour la norme que nous avons définie sur $\left(\frac{a,b}{F}\right)$, isométrie et isomorphisme d'algèbres sont synonymes, comme le montre le théorème suivant.

4.29 Théorème. Soient $A = \left(\frac{a,b}{F}\right)$ et $A' = \left(\frac{a',b'}{F}\right)$ avec $a, b, a', b' \in \dot{F}$. Alors les assertions suivantes sont équivalentes :

(a) A et A' sont isomorphes comme F-algèbres ;

(b) A et A' sont isométriques comme espaces quadratiques ;

(c) A_0 et A'_0 sont isométriques comme espaces quadratiques.

Avant de démontrer le théorème, il nous faut le lemme suivant.

4.30 Lemme. Si $A = \left(\frac{a,b}{F}\right)$, $A' = \left(\frac{a',b'}{F}\right)$ avec $a, b, a', b' \in \dot{F}$ et $\varphi : A \to A'$ est un *isomorphisme* de F-algèbres, alors $\varphi(A_0) = A'_0$.

Preuve. Il s'agit d'une conséquence directe de la caractérisation (4.25). En effet, si $v \in A_0$, alors $v \notin F$ et $v^2 \in F$, ce qui implique que $\varphi(v) \notin F$ et $\varphi(v)^2 \in F$. D'où $\varphi(A_0) \subseteq A'_0$.

Pour avoir l'inclusion inverse, on choisit un élément $\varphi(w) \in A'_0$ avec $w \in A$. On a alors $\varphi(w) \notin F$ et $\varphi(w)^2 \in F$, d'où on déduit directement $w \notin F$ et $w^2 \in F$, *i.e.* $w \in A_0$. □

Preuve de (4.29). Les assertions (b) et (c) se réécrivent comme

$$\begin{aligned} \text{(b)} \quad &\iff \quad \langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle, \\ \text{(c)} \quad &\iff \quad \langle -a, -b, ab\rangle \cong \langle -a', -b', a'b'\rangle. \end{aligned}$$

Dès lors, l'équivalence (b) $\Leftrightarrow$ (c) découle du théorème d'annulation de Witt.

Voyons que (a) $\Rightarrow$ (b). Soit $\varphi : A \to A'$ un isomorphisme de F-algèbres. Nous allons voir que φ est aussi une isométrie entre les espaces quadratiques A et A'. Il faut voir que pour tout $x \in A$,

$$N'(\varphi(x)) = N(x),$$

où N et N' sont les deux formes quadratiques associées à A et A' (*i.e.* les normes définies en (4.27)). Choisissons $x \in A$; il existe $\alpha \in F$ et $x_0 \in A_0$ tels que $x = \alpha + x_0$. On peut alors écrire

$$\varphi(x) = \alpha + \varphi(x_0) \quad \text{et} \quad \varphi(\overline{x}) = \alpha - \varphi(x_0).$$

Par le lemme (4.30), $\varphi(x_0) \in A'_0$, et ainsi nous avons $\overline{\varphi(x)} = \varphi(\overline{x})$. Cela nous permet de faire le calcul suivant :

$$N'(\varphi(x)) = \varphi(x) \cdot \overline{\varphi(x)} = \varphi(x) \cdot \varphi(\overline{x}) = \varphi(x\overline{x}) = \varphi(N(x)) = N(x).$$

Pour terminer la démonstration, voyons (c) $\Rightarrow$ (a). Soit $\sigma : A_0 \to A_0'$ une isométrie. On pose $\mathfrak{i} := \sigma(i)$ et $\mathfrak{j} := \sigma(j)$. On a que

$$\begin{aligned} \mathfrak{i}\bar{\mathfrak{i}} = N'(\mathfrak{i}) = N'(\sigma(i)) = N(i) = -a, \\ \mathfrak{j}\bar{\mathfrak{j}} = N'(\mathfrak{j}) = N'(\sigma(j)) = N(j) = -b, \\ N'(\mathfrak{ij}) = \mathfrak{ij}\overline{\mathfrak{ij}} = \mathfrak{i}(\mathfrak{j}\bar{\mathfrak{j}})\bar{\mathfrak{i}} = N(i)N(j) = ab. \end{aligned}$$

De plus, $\mathfrak{i}$, $\mathfrak{j}$ et $\mathfrak{ij}$ sont orthogonales deux-à-deux. En effet, en désignant par B (resp. B') la forme bilinéaire associée à la norme N (resp. N') sur A (resp. A'), on calcule

$$\begin{aligned} B'(\mathfrak{i},\mathfrak{j}) &= B'(\sigma(i),\sigma(j)) = \frac{1}{2}(N'(\sigma(i)+\sigma(j)) - N'(\sigma(i)) - N'(\sigma(j))) \\ &= \frac{1}{2}(N(i+j) - N(i) - N(j)) = 0, \end{aligned}$$

comme i et j sont orthogonales dans A. (On remarque, en passant, que $B'(\mathfrak{i},\mathfrak{j}) = 0$ est équivalent à $\mathfrak{ij} = -\mathfrak{ji}$.) Pour finir de voir l'orthogonalité, on calcule

$$B'(\mathfrak{ij},\mathfrak{j}) = \frac{1}{2}(\mathfrak{ij}\bar{\mathfrak{j}} + \mathfrak{j}\overline{\mathfrak{ij}}) = \frac{1}{2}(-\mathfrak{ijj} + \mathfrak{jji}) = \frac{1}{2}(-\mathfrak{jji} + \mathfrak{jji}) = 0,$$

et

$$B'(\mathfrak{ij},\mathfrak{i}) = \frac{1}{2}(\mathfrak{ij}\bar{\mathfrak{i}} + \mathfrak{i}\overline{\mathfrak{ij}}) = \frac{1}{2}(-\mathfrak{iji} + \mathfrak{iji}) = 0.$$

Ainsi, on obtient que $\mathfrak{i},\mathfrak{j},\mathfrak{ij}$ est une base (orthogonale) de A_0'. On peut définir un isomorphisme de F-espaces vectoriels $\beta : A \to A'$ par

$$\beta(1) = 1, \quad \beta(i) = \mathfrak{i}, \quad \beta(j) = \mathfrak{j} \quad \text{et} \quad \beta(k) = \mathfrak{ij}.$$

Grâce aux calculs que nous avons fait ci-dessus, on peut facilement vérifier qu'il s'agit en fait d'un isomorphisme de F-algèbres. □

4.31 Corollaire. Soit $a, b \in \dot{F}$ et $A = \left(\frac{a,b}{F}\right)$. Alors les assertions suivantes sont équivalentes :

(a) $A \cong \mathbb{M}_2(F)$ comme F-algèbres ;

(b) $\langle 1, -a, -b, ab\rangle$ est hyperbolique ;

(c) $\langle -a, -b, ab\rangle$ est isotrope.

PREUVE. '(a) $\Rightarrow$ (b)' En utilisant, (4.18) on a l'isomorphisme de F-algèbres

$$A \cong \left(\frac{-1,1}{F}\right),$$

d'où, par le théorème (4.29), l'isométrie d'espaces quadratiques

$$\langle 1,-a,-b,ab\rangle \cong \langle 1,1,-1,-1\rangle. \tag{4.32}$$

'(b) $\Rightarrow$ (c)' On a

$$\langle 1,-a,-b,ab\rangle \cong \langle 1,-1,1,-1\rangle \quad \Longrightarrow \quad \langle -a,-b,ab\rangle \cong \langle -1,1,-1\rangle,$$

par le théorème d'annulation de Witt.

'(c) $\Rightarrow$ (a)' Comme la forme quadratique $\langle -a,-b,ab\rangle$ est isotrope, il existe $q \in \dot{F}$ tel que

$$\langle -a,-b,ab\rangle \cong \langle 1,-1,q\rangle.$$

On a $(ab)^2 \cdot \dot{F}^2 = -q \cdot \dot{F}^2$, ce qui implique $q \cdot \dot{F}^2 = -1 \cdot \dot{F}^2$. Donc on obtient

$$\langle -a,-b,ab\rangle \cong \langle 1,-1,-1\rangle.$$

On retrouve ainsi (4.32), qui est équivalent à $A \cong \mathbb{M}_2(F)$ (comme F-algèbres), par le théorème (4.29). □

4.33 Corollaire. Soient $a,b,c,d \in \dot{F}$, alors

(a) $\left(\frac{a,b}{F}\right) \cong \left(\frac{b,a}{F}\right)$,

(b) $\left(\frac{a,b}{F}\right) \cong \left(\frac{ac^2,bd^2}{F}\right)$,

(c) $\mathbb{M}_2(F) \cong \left(\frac{1,1}{F}\right) \cong \left(\frac{1,a}{F}\right) \cong \left(\frac{b,-b}{F}\right) \cong \left(\frac{c,1-c}{F}\right)$, avec $c \neq 0,1$,

(d) $\left(\frac{a,a}{F}\right) \cong \left(\frac{a,-1}{F}\right)$.

PREUVE. *Partie* (a) : Comme on a

$$\langle 1,-a,-b,ab\rangle \cong \langle 1,-b,-a,ab\rangle,$$

on peut utiliser (4.29).

Partie (b) : De même, comme

$$\langle 1,-a,-b,ab\rangle \cong \langle 1,-ac^2,-bd^2,ac^2bd^2\rangle,$$

on peut utiliser (4.29).

Partie (c) : Pour pouvoir appliquer (4.31), on doit voir que les formes quadratiques suivantes sont isotropes :

$$\langle -1,-1,1\rangle, \quad \langle -1,-a,a\rangle, \quad \langle -b,b,-b^2\rangle, \quad \text{et} \quad \langle -c,c-1,c(1-c)\rangle.$$

Pour les trois premières, c'est immédiat. Pour montrer que la forme $\langle -c, c-1, c(1-c)\rangle$ est isotrope, on remarque d'abord qu'elle représente -1, et qu'ainsi il existe $r, s \in \dot{F}$ tels que

$$\langle -c,c-1,c(1-c)\rangle \cong \langle -1,r,s\rangle.$$

Comme

$$c^2(1-c)^2 \cdot \dot{F}^2 = -rs \cdot \dot{F}^2,$$

on a $s \cdot \dot{F}^2 = -r \cdot \dot{F}^2$. D'où

$$\langle -c,c-1,c(1-c)\rangle \cong \langle -1,r,-r\rangle,$$

qui est isotrope.

Partie (d) : Comme

$$\langle 1,-a\rangle \cong \langle -a,1\rangle \cong \langle -a,a^2\rangle,$$

on a l'isométrie

$$\langle 1,-a,1,-a\rangle \cong \langle 1,-a,-a,a^2\rangle.$$

Ce qui nous permet d'appliquer (4.29). □

4.34 Théorème (Linéarité). Pour tout $a, b, c \in \dot{F}$, on a l'isomorphisme de F-algèbres

$$\left(\frac{a,b}{F}\right) \otimes_F \left(\frac{a,c}{F}\right) \cong \left(\frac{a,bc}{F}\right) \otimes_F \left(\frac{c,-a^2c}{F}\right) \cong \left(\frac{a,bc}{F}\right) \otimes_F \mathbb{M}_2(F).$$

Preuve. En utilisant le corollaire (4.33), on a directement le deuxième isomorphisme. Le travail consistera donc seulement à montrer

$$\left(\frac{a,b}{F}\right) \otimes_F \left(\frac{a,c}{F}\right) \cong \left(\frac{a,bc}{F}\right) \otimes_F \left(\frac{c,-a^2c}{F}\right).$$

Soit $\{1,i,j,k\}$ et $\{1,i',j',k'\}$ les bases "standards" de $B = \left(\frac{a,b}{F}\right)$ et $C = \left(\frac{a,c}{F}\right)$. Avec elles, nous définissons deux nouvelles F-algèbres

$$X := F\cdot(1\otimes 1) + F\cdot(i\otimes 1) + F\cdot(j\otimes j') + F\cdot(k\otimes j'), \quad \text{et}$$
$$Y := F\cdot(1\otimes 1) + F\cdot(1\otimes j') + F\cdot(i\otimes k') + F\cdot(-ci\otimes i').$$

Il est facile de vérifier qu'il s'agit bien de sous-F-algèbres de $B \otimes_F C$ (de F-dimension 4). Dès lors, $X \otimes_F Y$ et $B \otimes_F C$ sont isomorphes en tant que F-espaces vectoriels car ils ont même dimension.

Pour construire un isomorphisme de F-espaces vectoriels "naturel" $\sigma : B \otimes_F C \to X \otimes_F Y$, on peut commencer par associer

$$\begin{aligned}
1 \otimes 1 &\longmapsto (1 \otimes 1) \otimes (1 \otimes 1),\\
i \otimes 1 &\longmapsto (i \otimes 1) \otimes (1 \otimes 1),\\
j \otimes j' &\longmapsto (j \otimes j') \otimes (1 \otimes 1),\\
k \otimes j' &\longmapsto (k \otimes j') \otimes (1 \otimes 1),\\
1 \otimes j' &\longmapsto (1 \otimes 1) \otimes (1 \otimes j'),\\
i \otimes k' &\longmapsto (1 \otimes 1) \otimes (i \otimes k'),\\
-ci \otimes i' &\longmapsto (1 \otimes 1) \otimes (-ci \otimes i').
\end{aligned}$$

De plus, comme il apparaît que les éléments

$$1 \otimes 1,\ \ i \otimes 1,\ \ j \otimes j',\ \ k \otimes j',\ \ 1 \otimes j',\ \ i \otimes k',\ \ -ci \otimes i'.$$

créent, par multiplication, une F-base de $B \otimes_F C$, on peut chercher à continuer la définition de σ sur la F-base engendrée en imposant la condition

$$\sigma(xy) = \sigma(x)\sigma(y), \quad \text{pour tout } x, y \text{ dans } B \otimes_F C. \tag{4.35}$$

On peut vérifier que σ ainsi défini est bien un isomorphisme de F-espaces vectoriels, qui de plus satisfait (4.35) et est donc un isomorphisme de F-algèbres. De cela, on obtient

$$B \otimes_F C \cong X \otimes_F Y,$$

en tant que F-algèbres. Ce qui déplace notre problème à prouver l'isomorphisme de F-algèbres

$$X \otimes_F Y \cong \left(\frac{a, bc}{F}\right) \otimes_F \left(\frac{c, -a^2c}{F}\right).$$

Pour ce faire, on commence par poser $I := i \otimes 1$ et $J := j \otimes j'$. On peut alors réécrire X :

$$X = F \cdot 1 + F \cdot I + F \cdot J + F \cdot (IJ), \quad (\text{avec } 1 = 1 \otimes 1),$$

et comme de plus

$$\begin{gathered}
I^2 = i^2 \otimes 1 = a(1 \otimes 1), \qquad J^2 = j^2 \otimes j'^{\,2} = bc(1 \otimes 1),\\
-IJ = -ij \otimes j' = ji \otimes j' = JI,
\end{gathered}$$

on peut construire un isomorphisme de F-algèbres entre X et $\left(\frac{a,bc}{F}\right)$.

Similairement, en posant $\widetilde{I} = 1 \otimes j'$ et $\widetilde{J} = i \otimes k'$, on peut montrer que $Y \cong \left(\frac{c,-a^2c}{F}\right)$, ce qui complète la preuve. □

4.36 Corollaire. Pour tout $a, b, c \in \dot{F}$, on a, dans $\mathrm{Br}(F)$,

$$\left[\left(\frac{a,b}{F}\right)\right] \cdot \left[\left(\frac{a,c}{F}\right)\right] = \left[\left(\frac{a,bc}{F}\right)\right] \quad \text{et} \quad \left[\left(\frac{a,b}{F}\right)\right] \cdot \left[\left(\frac{c,b}{F}\right)\right] = \left[\left(\frac{ac,b}{F}\right)\right],$$

et de plus

$$\left[\left(\frac{a,b}{F}\right)\right]^2 = 1_{\mathrm{Br}(F)}.$$

Preuve. Pour avoir les deux premières égalités, il suffit d'appliquer (4.34) (et (a) de (4.33)). Dès lors,

$$\left[\left(\frac{a,b}{F}\right)\right]^2 = \left[\left(\frac{a,b^2}{F}\right)\right] = \left[\left(\frac{a,1}{F}\right)\right] = \left[\left(\frac{1,a}{F}\right)\right] = [\mathbb{M}_2(F)] = 1_{\mathrm{Br}(F)},$$

où on a utilisé, dans l'ordre, (b), (a), et (c) de (4.33). □

Bibliographie

[1] Sheldon Axler, *Linear Algebra Done Right*, Springer, 1997.

[2] Steven Roman, *Advanced Linear Algebra*, Springer, 2008.

[3] Winfried Scharlau, *Quadratic and Hermitian Forms*, Springer, 1985.

[4] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, American Mathematical Society, 2005.

[5] Albrecht Pfister, *Quadratic Forms with Applications to Algebraic Geometry and Topology*, London Mathematical Society, 1995.